

**CENTRO UNIVERSITÁRIO DAS FACULDADES METROPOLITANAS UNIDAS  
PROGRAMA DE MESTRADO EM DIREITO DA SOCIEDADE DA INFORMAÇÃO**

**CRIMINALIDADE, PERSECUÇÃO PENAL E SOCIEDADE DA INFORMAÇÃO: A  
BUSCA PELA EFETIVIDADE ESTATAL**

**MARCELO NOGUEIRA NEVES**

**São Paulo  
2020**

**MARCELO NOGUEIRA NEVES**

**CRIMINALIDADE, PERSECUÇÃO PENAL E SOCIEDADE DA INFORMAÇÃO: A  
BUSCA PELA EFETIVIDADE ESTATAL**

Dissertação apresentada à Banca Examinadora das Faculdades Metropolitanas Unidas, como requisito parcial para obtenção do título de Mestre em Direito, sob a orientação da Profa. Dra. Greice Patrícia Fuller.

**São Paulo**

**2020**

Ficha catalográfica elaborada pela Biblioteca FMU  
com os dados fornecidos pelo(a) autor(a)

Nc Nogueira Neves, Marcelo  
Criminalidade, persecução penal e sociedade da informação:  
A busca pela efetividade estatal / Marcelo Nogueira Neves;  
orientadora Greice Patricia Fuller. -- São Paulo, 2020.  
134 p.

Dissertação (Mestrado - Direito da Sociedade da  
Informação) -- Faculdades Metropolitanas Unidas, 2020.

1. Sociedade da informação;. 2. Crimes Cibernéticos; . 3.  
Persecução Penal; . 4. Tutela Estatal.. I. Patricia Fuller, Greice,  
orient. II. Título.

**MARCELO NOGUEIRA NEVES**

**CRIMINALIDADE, PERSECUÇÃO PENAL E SOCIEDADE DA INFORMAÇÃO: A  
BUSCA PELA EFETIVIDADE ESTATAL**

Data da aprovação:

\_\_\_\_ / \_\_\_\_ / \_\_\_\_

Banca examinadora:

---

Profa. Dra. Greice Patrícia Fuller  
Orientadora

---

Prof. Dr. Irineu Francisco Barreto Junior  
Examinador

---

Prof. Dr. Roberto Ferreira Archanjo da  
Silva  
Examinador

**São Paulo**

**2020**

Àquela que está sempre ao meu lado em todos os momentos, parte indiscutível desta conquista, e que faz cada dia valer a pena, minha amada esposa.

## **AGRADECIMENTOS**

À orientadora e amiga, Professora Doutora Greice Patrícia Fuller, pela confiança em mim depositada, pelos ensinamentos e contribuições brilhantes, pelo apoio e paciência de sempre.

Aos meus pais Onofre e Rosa, por tudo que fizeram por mim e meus irmãos, que de onde estiverem, recebem minha gratidão eterna.

Aos meus irmãos Márcia e Maurício, pela preocupação e incentivo, por jamais esquecerem da conexão que há entre irmãos.

Ao meu filho Marcelo, responsável por fazer-me sentir o verdadeiro amor entre pai e filho.

Aos demais Professores do Mestrado, pela dedicação e por todo o conhecimento transmitido.

Aos amigos que fiz ao longo desses dois anos, por contribuírem para tornar essa jornada uma realidade.

À Stefani, secretária do Mestrado, pela presteza e gentileza de sempre.

## RESUMO

O trabalho tem como principal objetivo demonstrar que o enfrentamento aos crimes cibernéticos e os mecanismos que hoje existem para a contenção desta modalidade criminosa estão se mostrando insuficientes para a efetividade da tutela estatal. Referida análise demonstrará que os riscos decorrentes do avanço tecnológico são iminentes, reclamando a necessidade de uma adequação do Direito Penal e do Direito Processual Penal com o objetivo de identificar e responsabilizar aqueles que fazem uso da tecnologia como um instrumento para a prática delituosa. A pesquisa foi pautada nos métodos dedutivo e jurídico descritivo, com a pesquisa bibliográfica e documental sobre o tema. O estudo é concluído com uma reflexão sobre os desafios da sociedade brasileira no enfrentamento aos crimes cibernéticos, demonstrando que as lacunas hoje existentes no ordenamento jurídico penal brasileiro demandam maior atenção não somente do poder legislativo, mas também de todos os operadores do direito, com o objetivo de melhor adequar as condutas delitivas praticadas na *internet*, tornando o Estado mais atuante e eficiente, e deixando de existir a sensação de impunidade que hoje predomina.

Palavras-chave: Sociedade da Informação; Crimes Cibernéticos; Persecução Penal; Tutela Estatal.

## **ABSTRACT**

The main objective of this paper is to demonstrate that the fight against cybercrimes and the mechanisms that exist today to contain this criminal modality are proving insufficient for the effectiveness of state protection. Said analysis will demonstrate that the risks arising from technological advances are imminent, claiming the need for an adaptation of Criminal Law and Criminal Procedural Law in order to identify and hold those responsible who use technology as an instrument for criminal practice. The research was based on deductive and legal descriptive methods, with bibliographic and documentary research on the topic. The study concludes with a reflection on the challenges facing Brazilian society in tackling cybercrimes, demonstrating that the gaps that currently exist in the Brazilian criminal legal system demand greater attention not only from the legislative branch, but also from all legal operators, with the objective of better adapting the criminal conduct practiced on the internet, making the State more active and efficient, and ceasing to exist the feeling of impunity that prevails today.

Key-words: Information Society; Cybercrimes; Criminal Prosecution; State Guardianship.



## SUMÁRIO

Introdução.....	10
1 – Crimes cibernéticos.....	15
1.1 Conceituação de crimes cibernéticos e aspectos gerais sobre sua tipificação penal.....	21
1.2 <i>Internet versus</i> criminalidade: superexposição e vulnerabilidade dos usuários.....	27
1.2.1 A responsabilidade ético-social em face do convívio no ambiente virtual.....	30
1.2.2 Responsabilidade <i>versus</i> liberdade de expressão.....	35
1.3 Ofensividade <i>on-line</i> e responsabilização penal.....	38
1.3.1 A Morte social como extensão do dano.....	39
1.3.2 Responsabilização penal por compartilhamento de conteúdo.....	43
2 – Criminalidade na Sociedade da Informação: desafios no enfrentamento e a busca pela efetividade estatal.....	48
2.1 Estabelecimento da jurisdição e da competência nos crimes cibernéticos.....	48
2.1.1 Extraterritorialidade e transnacionalidade.....	52
2.1.2 Competência em território nacional.....	55
2.2 Ambiente virtual e prova: desafios na colheita do conjunto probatório.....	59
2.2.1 Meios de obtenção da prova no ambiente virtual.....	63
2.2.1.1 Interceptação cibernética.....	63
2.2.1.2 Infiltração no ambiente virtual.....	64
2.2.1.3 Busca e apreensão cibernética.....	68
2.2.1.4 O Marco Civil da <i>Internet</i> e a obtenção da prova digital.....	68
2.2.1.5 Aplicações de comunicação instantânea.....	72
2.2.1.6 Cooperação internacional.....	76
2.2.2 <i>Deep Web</i> e <i>Dark Web</i> .....	79
2.2.2.1 Navegação anônima – TOR.....	81
2.2.2.2 <i>Bitcoin</i> e <i>Dark Web</i> .....	84
2.2.2.3 Criminalidade na <i>Dark Web</i> .....	85

3 – Instrumentos aditivos ao enfrentamento dos crimes cibernéticos.....	89
3.1 Educação digital: políticas públicas para o uso responsável da <i>internet</i> .....	89
3.2 Processo legislativo: reavaliação e adequação de condutas e tipos penais.....	94
3.3 Convenção de Budapeste: a adesão do Brasil como alternativa ao enfrentamento dos crimes cibernéticos.....	99
 Conclusão.....	 109
 Referências.....	 116
 Anexo A – Imagens ilustrativas da navegação na <i>Dark Web</i> .....	 123

## Introdução

A forma como as pessoas estabelecem a comunicação tem passado por diversas alterações no decorrer dos tempos, gerando transformações significativas na forma como se dá o acesso à informação, aprimorando e facilitando os meios para se comunicarem. Houve um tempo em que a escrita era a forma definida, e a carta era a principal ferramenta disponível para estabelecer a comunicação. Posteriormente surgiu o telefone, o que alterou completamente a forma como as pessoas se comunicavam. Em paralelo ao surgimento do telefone, as rádios surgiram como meio inovador de levar-se a informação para várias pessoas ao mesmo tempo, surgindo então a comunicação em massa. Posteriormente, com o surgimento da televisão, além da possibilidade da comunicação alcançar um número ainda maior de pessoas, esta passou a transmitir não apenas sons, mas também imagens, o que revolucionou a forma de se comunicar.

Na atualidade, os meios de comunicação encontram-se num patamar altamente tecnológico, e nunca tivemos a nossa disposição ferramentas tão ágeis e fáceis de lidar para o único e exclusivo propósito de se comunicar. Toda tecnologia envolvida atualmente nos meios de comunicação gerou o surgimento da denominada Sociedade da Informação, onde a disseminação e o acesso à informação desempenha um papel fundamental para o desenvolvimento da sociedade, inserindo por completo cada indivíduo no processo das comunicações pessoais, de trabalho, e de lazer, proporcionando bem estar e qualidade de vida.

Os impactos gerados pelo avanço tecnológico e a facilidade de acesso a informação são, indiscutivelmente, extremamente positivos diante do contexto da globalização, porém a tecnologia que tanto auxilia o cotidiano das pessoas, acaba por expô-las aos riscos das condutas de pessoas mal intencionadas, que buscam na tecnologia a oportunidade de praticarem crimes, os já popularmente conhecidos crimes cibernéticos, crimes virtuais ou ainda crimes informáticos.

O enfrentamento à criminalidade cibernética tornou-se um dos maiores desafios da atualidade, e para minimizar seus efeitos deverá o Estado realizar investimentos contínuos para a capacitação adequada de seus agentes, bem como a aquisição de equipamentos de última geração e tecnologia de ponta, e acima de tudo, primordial que sejam executadas políticas públicas voltadas a educação e conscientização do uso adequado da *internet*, promovendo em cada usuário a

consciência de uma navegação responsável na rede. Deve-se considerar ainda uma melhor adequação legislativa para a tipificação das condutas ilícitas que são praticadas através da *internet*, elaborando-se um conjunto de leis que atenda a atual demanda, mantendo-as atualizadas para que as respostas ao enfrentamento dos crimes cibernéticos sejam alcançadas.

A sociedade brasileira está diante de um grande desafio, e as lacunas que hoje existem no ordenamento jurídico penal brasileiro demandam maior atenção não somente do poder legislativo, mas também de todos os operadores do direito, com o intuito de haver uma melhor adequação das condutas hoje praticadas através da *internet*, tornando o Estado mais atuante e deixando de existir a sensação de impunidade que hoje é predominante.

O conteúdo da presente pesquisa procura conhecer os principais pontos atinentes ao enfrentamento dos crimes cibernéticos, bem como os mecanismos que hoje está disponível para a contenção desta modalidade criminosa. Ao longo do trabalho serão apresentadas razões que justificarão que os mecanismos de enfrentamento estão se mostrando insuficientes para a efetividade da tutela estatal, analisando-se ainda o quadro atual da persecução penal relacionado aos crimes cibernéticos, e gerando uma reflexão sobre a importância da reavaliação das tipificações penais onde os crimes são praticados na *internet*, bem como da reavaliação dos procedimentos processuais penais para o seu efetivo enfrentamento.

Para atingir seus objetivos, a pesquisa foi pautada nos métodos dedutivo, jurídico descritivo e dialético, buscando-se a pesquisa bibliográfica sobre o tema dos crimes cibernéticos, através de obras literárias, artigos científicos, boletins, jornais, revistas, dissertações, também através de pesquisa documental jurídica, abrangendo o conhecimento pela ciência jurídica através da legislação, doutrina e jurisprudência, além de uma análise crítica do objeto pesquisado, com a contextualização da problemática envolvendo a cibercriminalidade.

O primeiro capítulo abordará o estudo da criminalidade informática, e será feita a análise do ambiente digital e as facilidades que os criminosos encontram para a prática de crimes, isto devido às características peculiares desta modalidade criminosa. Estudará os principais tipos penais infringidos por meio do ambiente digital, demonstrando-se que não há em suas descrições a utilização do computador e/ou outros dispositivos com acesso à *internet* como meio para o cometimento dos crimes, o que os tornam crimes comuns, sem qualquer previsão legal do agravamento da

lesão em virtude de serem praticados em ambiente digital. Neste sentido, serão avaliados ainda os institutos da Suspensão Condicional do Processo, da Transação Penal e da Prescrição frente aos crimes cibernéticos.

A responsabilidade será objeto de estudo, avaliando-se o comportamento dos usuários ao acessar a *internet*, inclusive as responsabilidades que decorrem do exercício do direito à liberdade de expressão, avaliando-se também os limites do exercício deste direito frente a outros direitos fundamentais e de mesma hierarquia. Ressalta-se ainda a predominância de uma superexposição dos usuários na rede, que quando estão conectados, extrapolam o compartilhamento de informações de suas vidas privadas, gerando riscos e tornando-os vulneráveis, o que poderia ser evitado com a maior conscientização e a adoção de cuidados mínimos de segurança.

O estudo da morte social como extensão do dano será abordado com o objetivo de demonstrar o quão danosa se mostra uma conduta praticada através da *internet*, gerando consequências muitas vezes irreversíveis àquelas vítimas que diante dos meios que hoje dispõem não conseguiram cessar os desdobramentos do dano.

Encerrando o primeiro capítulo, a responsabilidade penal pelo compartilhamento de conteúdo ilícito através da *internet* e sua adequada tipificação penal serão também estudadas, com o objetivo de dar maior entendimento ao que na atualidade tem se tornado muito comum, o compartilhamento indiscriminado de conteúdo sem a adoção de critérios mínimos de verificação quanto a sua licitude e veracidade, abrangendo inclusive alguns aspectos relacionados às *fake news*.

O segundo capítulo abordará o estudo de uma das questões mais desafiadoras quanto a persecução penal dos crimes cibernéticos, que é a correta determinação da jurisdição e da competência, isto em razão dessas espécies de crimes possuírem a peculiar característica da plurilocalidade, podendo atingir ainda a transnacionalidade, o que implicará necessariamente na colaboração de um país estrangeiro para o êxito das investigações. A aplicação da lei processual penal no tempo e no espaço frente aos crimes praticados na *internet* será objeto de estudo, demonstrando o grande desafio existente diante do fato de não existirem barreiras físicas no ambiente virtual, o que demanda dos órgãos de investigação cuidados extras na execução de seu trabalho.

Será estudado ainda mais um dos grandes obstáculos enfrentados pelos agentes públicos no enfrentamento à cibercriminalidade, que é a busca pela apuração

e colheita de um conjunto probatório satisfatório e que venha contribuir para a identificação e punição dos criminosos cibernéticos. A prova a ser buscada, que antes deixava vestígios físicos, agora ocupa o ambiente virtual, gerando maior dificuldade na sua apuração e tornando-se mais suscetíveis ao perecimento. Serão estudados os meios de obtenção de prova disponíveis para aplicação nas investigações cibernéticas, como a interceptação cibernética, a infiltração de agentes no ambiente digital, a busca e apreensão cibernética, além de aspectos gerais sobre as previsões legais trazidas pelo Marco Civil da *Internet*. O estudo das aplicações de comunicação instantânea como importante meio de obtenção de prova também será abordado, isto em razão de a grande maioria dos usuários da *internet* fazerem uso deste tipo de aplicação.

A *Deep Web* e a *Dark Web* também farão parte do objeto de estudo do segundo capítulo, onde será mais bem esclarecido como os criminosos fazem uso deste meio de navegação para tentar burlar a investigação e manterem-se impunes. Este tópico será composto por alguns “*prints*” de tela, com o objetivo de ilustrar o ambiente virtual frequentado pelos criminosos, e que demonstram o quão complexo e desafiador é a identificação dos autores dos crimes cibernéticos nesta área de navegação da *internet*.

Por fim, serão estudados alguns mecanismos que poderão ser adotados para auxiliar o enfrentamento dos crimes cibernéticos, tais como a educação digital, ressaltando a importância da adoção de políticas públicas que venham contribuir para que os usuários da *internet* façam seu uso de forma segura e consciente. Além do papel relevante que a educação tem nesse processo de enfrentamento aos crimes cibernéticos, será tratada ainda a possibilidade de que seja revisto o ordenamento jurídico penal brasileiro quanto à prática de crimes praticados na *internet*, passando pelo processo de adequação legislativa, não somente no direito material, mas também no que tange o direito processual penal. Derradeiramente será objeto de estudo a adesão do Brasil à Convenção de Budapeste, já que a colaboração entre países, além da tipificação de algumas condutas praticadas na *internet* fazem parte do conteúdo da referida Convenção, o que colocaria o país num patamar internacional na adoção de mecanismos no enfrentamento aos crimes cibernéticos.

Diante de toda a problemática existente em encontrar os melhores meios para o enfrentamento aos crimes cibernéticos, deverá o Estado prestar sua tutela com o objetivo de melhor enfrentar esta modalidade criminosa e que aflige toda sociedade

brasileira, identificando seus autores, punindo-os e por consequência minimizando os danos causados.

## 1 – Crimes cibernéticos

A Sociedade da Informação é responsável por uma grande mudança no comportamento social mundial, e o avanço tecnológico está alterando a forma como as pessoas vivem. A disseminação e o compartilhamento de informações através do uso cada vez mais frequente da *internet* refletem diretamente nas questões sociais, políticas e econômicas de um país.

Ao conceituar Sociedade da Informação, Roberto Senise Lisboa ensina que:

“Sociedade da informação”, também denominada de “sociedade do conhecimento”, é expressão utilizada para identificar o período histórico a partir da preponderância da informação sobre os meios de produção e a distribuição dos bens na sociedade, que se estabeleceu a partir da vulgarização das programações de dados utilizados nos meios de comunicação existentes e dos dados obtidos sobre uma pessoa e/ou objeto, para a realização de atos e negócios jurídicos. Não se limita a sociedade da informação, pois, ao computador ou a um direito informático, já que estende-se a qualquer meio de comunicação, presencial ou não. Assim, por exemplo: a televisão a cabo, por antena ou via satélite; o *teleshopping*, o *teleshopping* e o *teleworking*; o rádio e o telefone.<sup>1</sup>

O Brasil, obviamente, não poderia ficar indiferente a esta relevante mudança comportamental do mundo contemporâneo, e neste contexto, o Livro Verde, organizado por Tadao Takahashi e lançado pelo Ministério da Ciência e Tecnologia no ano de 2000, contemplou um conjunto de ações para impulsionar a sociedade da informação no Brasil em todos os seus aspectos, descrevendo que:

Assistir à televisão, falar ao telefone, movimentar a conta no terminal bancário e, pela Internet, verificar multas de trânsito, comprar discos, trocar mensagens com o outro lado do planeta, pesquisar e estudar são hoje atividades cotidianas, no mundo inteiro e no Brasil. Rapidamente nos adaptamos a essas novidades e passamos – em geral, sem uma percepção clara nem maiores questionamentos – a viver na Sociedade da Informação, uma nova era em que a informação flui a velocidades e em quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais.<sup>2</sup>

Os jovens, ainda na mais tenra idade, se interessam cada vez mais pela tecnologia inserida nos equipamentos de informática, o que lhes concede pleno acesso ao mundo virtual, e já é bastante comum que inclusive bebês manejem

<sup>1</sup> LISBOA, Roberto Senise. **Direito na sociedade da informação**. São Paulo: Revista dos Tribunais, 2006, p. 10. Disponível em: [https://scholar.google.com.br/citations?user=85XbR84AAAAJ&hl=pt-BR#d=gs\\_md\\_cita-d&u=%2F citations%3Fview\\_op%3Dview\\_citation%26hl%3Dpt-BR%26user%3D85XbR84AAAAJ%26citation\\_for\\_view%3D85XbR84AAAAJ%3AzYLM7Y9cAGgC%26tzm%3D180](https://scholar.google.com.br/citations?user=85XbR84AAAAJ&hl=pt-BR#d=gs_md_cita-d&u=%2F citations%3Fview_op%3Dview_citation%26hl%3Dpt-BR%26user%3D85XbR84AAAAJ%26citation_for_view%3D85XbR84AAAAJ%3AzYLM7Y9cAGgC%26tzm%3D180). Acesso em: 08 out. 2020.

<sup>2</sup> TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000, p.3.



equipamentos eletrônicos (o que parece, de forma bastante precoce). Por outro lado, os senis, que há pouco tempo se posicionavam de forma avessa aos “encantos” da tecnologia, já estão encarando as mudanças com maior naturalidade e já se rendem às facilidades que o mundo digital lhes proporcionam.

Neste sentido, como ensinam Damásio de Jesus e José Antonio Milagre:

É inerente a esta sociedade que o acesso livre às tecnologias e à rede seja um direito de todos os cidadãos. Mais do que isso, garantias e liberdades constitucionais passam a ser consideradas e refletidas à luz dos impactos que as novas tecnologias trazem no dia a dia. Nas escolas, no trabalho ou nas relações pessoais, estar *online* é realidade, não no mero contexto de estar conectado, mas no sentido de estar incluído digitalmente, algo além do tradicional ler e escrever, diga-se, ser um ser social digital, estar em “rede”.<sup>3</sup>

O que se constata é que a tecnologia que hoje está inserida nos equipamentos de informática, que aliada ao acesso à *internet*, possibilita com que as pessoas tenham acesso à informação, apesar de todos os problemas relacionados à exclusão digital no país, onde uma grande parcela da população ainda não dispõe de acesso aos benefícios tecnológicos.

O que antes era possível apenas através de um computador sobre a mesa, agora é alcançado através de dispositivos móveis, como *smartphones*, *notebooks* e *tablets*, que ganharam a preferência ao redor do mundo, e sua portabilidade, aliada à capacidade de acesso e à facilidade de compartilhamento de informações, fazem destes os objetos de desejo da sociedade moderna, proporcionando o acesso ao ambiente digital, e conseqüentemente contribuindo substancialmente para a inserção do indivíduo na sociedade.

Ao tratar da disseminação da *internet* na Sociedade da Informação, Irineu Francisco Barreto Junior ensina que:

Esta nova era apresenta, como marco inicial, a ruptura dos padrões de sociabilidade típicos do Século XX, provocada por uma série de eventos sistêmicos e concatenados em escala mundial, aos quais se convencionou denominar como Sociedade da Informação. Inaugura-se um novo estágio do modo de produção capitalista, instaurado pela convergência tecnológica e digital, pelo exponencial crescimento – e conseqüente diminuição dos custos – da produção de equipamentos informáticos e, principalmente, pela disseminação em escala mundial da Internet.<sup>4</sup>

<sup>3</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 17.

<sup>4</sup> BARRETO JUNIOR, Irineu Francisco. Proteção de dados pessoais na *internet*: o marco civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 406.

Segundo a 31ª Pesquisa Anual de Administração e Uso de Tecnologia da Informação nas Empresas<sup>5</sup>, divulgada pela Fundação Getúlio Vargas no ano de 2020, no Brasil já são aproximadamente 430 (quatrocentos e trinta) milhões de aparelhos desse tipo, permitindo com que as pessoas tenham acesso ao mundo da *internet*. Levando em conta que a população do país é de aproximadamente 209 (duzentos e nove) milhões de pessoas, os números são significativos.

Já o relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento<sup>6</sup> (UNCTAD) emitido no ano de 2017, coloca o Brasil como o quarto país com maior número de usuários de *internet*, ficando atrás somente dos Estados Unidos, Índia e China. E ainda, a Pesquisa Nacional por Amostra de Domicílio<sup>7</sup>, PNAD Contínua, realizada pelo IBGE em 2018, indicou um aumento considerável do número de pessoas que acessam a *internet* no Brasil, alcançando a porcentagem de 74,7% da população com idade a partir dos 10 anos de idade.

A inovação tecnológica de que hoje dispomos está determinando importantes transformações culturais e sociais. As pessoas de onde estiverem acessam documentos, realizam operações financeiras e comerciais, e ainda usufruem de uma infinidade de entretenimento em diversas áreas, comunicando-se com outros usuários da rede sem qualquer tipo de limitação.

Como ensina Zygmunt Bauman sobre o fato das pessoas sentirem-se inseridas no mundo:

A chegada da internet pôs ao alcance de cada fulano, beltrano e sicrano um feito que antes exigia as incursões noturnas de uns poucos grafiteiros treinados e aventureiros: transformar o invisível em visível, tornando gritante e dissonantemente presente o negligenciado, ignorado e abandonado – em suma, torna tangível e irrefutável o ser e o estar no mundo.<sup>8</sup>

O acesso às novas culturas, idiomas, países, e religiões, nos inserem totalmente no mundo globalizado, e este novo cenário de tecnologias da informação e comunicação contribui para a integração plena dos seres humanos. E ainda, no que

---

<sup>5</sup> FGV. **31ª Pesquisa Anual de Administração e Uso de Tecnologia da Informação nas Empresas/2020**. Disponível em: [https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados\\_0.pdf](https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados_0.pdf). Acesso em: 08 out. 2020.

<sup>6</sup> ONU. **UNCTAD 2017 – United nations conference on trade and development**. Disponível em: [https://unctad.org/en/PublicationsLibrary/wir2017\\_en.pdf](https://unctad.org/en/PublicationsLibrary/wir2017_en.pdf). Acesso em 25 jul. 2019.

<sup>7</sup> IBGE. **PNAD 2018 - Pesquisa Nacional por Amostra de Domicílio**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/27515-pnad-continua-tic-2018-internet-chega-a-79-1-dos-domicilios-do-pais>. Acesso em: 08 out. 2020.

<sup>8</sup> BAUMAN, Zygmunt; DAVID, Lyon. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013, p. 20.

Bauman<sup>9</sup> ensina como sendo o mundo pós-pan-óptico da sociedade líquida moderna, as informações são disponibilizadas na *internet* por todos os que compram, buscam entretenimento, e fazem uso de seus *smartphones*, o que acaba gerando aos usuários algum tipo de punição.

Não restam dúvidas de que o avanço tecnológico que estamos vivenciando e a facilidade de acesso a toda essa tecnologia acaba por gerar diversos impactos na sociedade, tanto os positivos quanto os negativos. É evidente que as facilidades que o acesso à informação traz são extremamente úteis em todos os contextos, onde todos buscam estar atualizados e conectados com o restante do mundo. Porém, a tecnologia que tanto auxilia o cotidiano das pessoas, acaba por expô-las aos riscos das condutas daqueles que buscam o acesso à tecnologia não para fazerem parte de um mundo que busca o seu aperfeiçoamento através da informação, mas sim para a prática de crimes, os já popularmente conhecidos crimes cibernéticos, crimes virtuais ou ainda crimes informáticos.

Quanto aos riscos que a sociedade da informação proporciona aos seus usuários, Jesus e Milagre ensinam:

E a sociedade da informação (ou para muitos, pós-industrial) tem, sim, seus riscos. Pode ser chamada de sociedade dos riscos. Riscos que podem ser aceitos e riscos que devem ser mitigados. E um deles está associado à criminalidade digital. Ao considerarmos que nem todo cidadão decidiu ingressar mas lançado foi no universo digital, constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos (...)<sup>10</sup>

Relatório emitido pela empresa Norton Cyber Security<sup>11</sup>, em 2018, e que avaliou a incidência dos crimes cibernéticos em 16 (dezesesseis) países do mundo, dentre eles o Brasil, indica que mais de 1 (um) bilhão de pessoas já se tornaram vítimas de cibercriminosos, sendo que destes, mais de 860 (oitocentos e sessenta) milhões de pessoas apenas no ano de 2017. De acordo com o relatório, no Brasil, e no mesmo ano, 70 (setenta) milhões de pessoas foram vítimas de crimes cibernéticos, alcançando um número total de 89 (oitenta e nove) milhões de pessoas vitimadas.

O campo para a atuação dos criminosos é vasto, pois dadas as características do ambiente digital, não há limites territoriais ou qualquer outro tipo de barreira física,

<sup>9</sup> BAUMAN, Zygmunt; DAVID, Lyon. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013, p. 121.

<sup>10</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 19.

<sup>11</sup> NORTON. **Norton cyber security insights report global results 2018**. Disponível em: [https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018\\_Norton\\_LifeLock\\_Cyber\\_Safety\\_Insights\\_Report\\_US\\_Media\\_Deck.pdf?promocode=DEFAULTWEB%20](https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_US_Media_Deck.pdf?promocode=DEFAULTWEB%20). Acesso em: 08 out. 2020.

e uma simples ação criminosa pode atingir um número inestimável de pessoas, podendo abranger inclusive diversos países, causando danos em níveis muito elevados.

Na medida em que as pessoas divulgam através da rede suas informações pessoais, imagens, vídeos, pensamentos ideológicos, convicções religiosas, partidarismo político, opções sexuais, etc., proporcionam que essas informações sejam utilizadas de maneira ilícita contra os próprios que as divulgaram. A superexposição na rede e o fácil acesso e compartilhamento de informações proporcionam ambiente fértil para a prática de ilícitos na *internet*, o que afronta direitos constitucionalmente tutelados, como a honra, a intimidade e a privacidade, razão pela qual a atuação penal não pode ser marginalizada.

A ausência de barreiras físicas no ambiente digital e o anonimato dos criminosos, que é obtido através de recursos técnicos que dificultam sua identificação, aliadas à velocidade da evolução tecnológica, constituem obstáculos à persecução penal e fazem deste um dos maiores desafios da atualidade. Há a necessidade permanente de o Estado realizar investimentos para a capacitação adequada de seus agentes, a aquisição de equipamentos de última geração e tecnologia de ponta, para que os criminosos deixem de se sentir tão confortáveis no ambiente digital e possam ser identificados e punidos.

O ambiente digital, além da sensação de anonimato que ele proporciona, gera um distanciamento natural das pessoas, por deixarem de se relacionar no ambiente físico. Por consequência, muitas pessoas passam a adotar condutas ilícitas em virtude da impessoalidade que a *internet* lhes proporciona. Conforme Zygmunt Bauman<sup>12</sup> ensina, com o avanço digital as relações tidas como tradicionais, e que deveriam ainda existir entre as pessoas foram afastadas, e o sujeito passa a ser incapaz de visualizar a vítima, tornando a prática do crime mais fácil, impessoal.

O distanciamento entre as pessoas e o sentimento de anonimato, inerentes ao ambiente digital, contribuem para que um número maior de pessoas venham praticar algum tipo de ilícito, e estar-se-á portanto, diante da multiplicidade de sujeitos ativos, ou o que Greice Patrícia Fuller<sup>13</sup> ensina como sendo a criminalidade difusa.

---

<sup>12</sup> BAUMAN, Zygmunt. **Globalização: as consequências humanas**. Rio de Janeiro: Jorge Zahar, 1999, p. 24.

<sup>13</sup> FULLER, Greice Patrícia. O Direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. **VII Congresso brasileiro da sociedade da informação regulação da mídia na sociedade da informação**, 2014, p. 137.

Esse fenômeno acarreta a dificuldade ainda maior de identificar quem é o sujeito ativo numa determinada conduta penalmente prevista, gerando por consequência a ineficácia ou a improdutividade das fases de investigação, e conseqüentemente, a persecução penal deixará de ser efetiva da forma como se espera. Como se observa na decisão descrita a seguir:

PENAL. PROCESSUAL PENAL. RECURSO EM SENTIDO ESTRITO. CRIME CONTRA A HONRA. CALÚNIA. COMPARTILHAMENTO DE NOTÍCIA ALEGADAMENTE FALSA EM REDE SOCIAL. IRRESIGNAÇÃO QUANTO À SENTENÇA QUE DECLAROU EXTINTA A PUNIBILIDADE DO QUERELADO, POR NÃO TER O QUERELANTE DEMANDADO CONTRA TODOS QUE VEICULARAM A NOTÍCIA CALUNIOSA. RENÚNCIA TÁCITA. INDIVISIBILIDADE DA AÇÃO PENAL PRIVADA. SELETIVIDADE DEMONSTRADA. RENÚNCIA TÁCITA QUE A TODOS SE IMPÕE. 1 – Demonstrado nos autos que o querelante optou por demandar apenas contra uma parte das pessoas que "compartilharam" a notícia caluniosa, ao tempo em que colacionou nos autos uma ata notarial relacionando todos que praticaram a conduta, incorreu em renúncia tácita, agindo seletivamente. Precedentes do STF. 2 – Sentença que merece ser mantida por seus próprios fundamentos. 3 – Recurso conhecido e improvido.(TJ-AL - RSE: 07010282020168020082 AL 0701028-20.2016.8.02.0082, Relator: Des. Washington Luiz D. Freitas, Data de Julgamento: 20/03/2019, Câmara Criminal, Data de Publicação: 22/03/2019).<sup>14</sup>

Na criminalidade difusa não se pode ignorar a dificuldade que há em conhecer-se todos os autores da fato, o que implica em real obstáculo à persecução penal, levando à conclusão da necessidade de se considerar as novas implicações existentes no ambiente digital em decorrência de crimes cibernéticos. Fuller ainda ensina que:

(...) a criminalidade difusa mediática praticada no contexto do meio ambiente digital ofende a dignidade da pessoa humana, quer com a invasão do direito à intimidade e privacidade; quer com a informação abusiva ou leviana (por falta de elementos probatórios fáticos e jurídicos); quer com informações que apregoem o 'discurso do ódio' (hate speech); quer com qualquer outra informação que viole direitos e garantias constitucionais fundamentais, como v.g. imagem, honra, intimidade, vida, dentre outros.<sup>15</sup>

Além de todos os aspectos abordados até aqui, deve-se considerar ainda uma adequação legislativa para a tipificação das condutas ilícitas praticadas através da *internet*. Muitos crimes cibernéticos já são processados e julgados através de leis que já vigem no nosso ordenamento jurídico penal, sendo a *internet* considerada apenas um meio para a prática delituosa, porém o que se deixa de apreciar com a ausência

<sup>14</sup> BRASIL. Superior Tribunal de Justiça. **RSE – 07010282020168020082 AL 0701028-20.2016.8.02.0082**. Disponível em: <https://tj-al.jusbrasil.com.br/jurisprudencia/689268082/recursoem-sentido-estrito-rse7010282020168020082-al-0701028-2020168020082/inteiro-teor-689268091>. Acesso em: 06 abr. 2019.

<sup>15</sup> FULLER, Greice Patrícia. O Direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. **VII Congresso brasileiro da sociedade da informação regulação da mídia na sociedade da informação**, 2014, p. 137.

de tipificações específicas é a desproporcionalidade do dano causado por um crime praticado no ambiente digital quando comparado à mesma conduta praticada no ambiente físico. Conclui-se, por certo, que a proporção do dano será infinitamente maior naquele quando comparada a este.

Diante de toda a problemática que vivemos, deverá o Estado prestar sua tutela no sentido de enfrentar esta modalidade criminosa e que aflige todo o mundo contemporâneo, identificando seus autores, punindo-os e por consequência minimizando os danos causados. Jesus e Milagre ainda ensinam:

Não podemos aceitar que na sociedade da informação vigore a lei de talião, autotutela ou a lei do mais forte, mas é sabido que o Direito deve prevalecer, fazendo valer a justiça nos conflitos entre cidadãos desta sociedade digital. Faz-se preciso o mínimo de controle para fazer frente àquele que realiza uma conduta antissocial cibernética. Ser internauta não é delito, assim como ser cidadão não é infração criminal, mas ambos, internauta ou cidadão, podem praticar, sim, infrações. É cediço que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Ninguém pode ser responsabilizado por fato que a lei desconsidera como de relevância penal.<sup>16</sup>

Neste sentido, estaria o Estado Brasileiro prestando a efetiva tutela no enfrentamento aos crimes cibernéticos? Dispõe a legislação Penal Brasileira de mecanismos suficientes para atender esta demanda? Jesus e Milagre<sup>17</sup> ainda ressaltam que o processo legislativo muito provavelmente não acompanhará os avanços na áreas da tecnologia, não significando que os profissionais do direito devem se manter omissos, aguardando providências do poder legislativo na elaboração de leis que atendam as demandas geradas pelos crimes cibernéticos. Segundo os autores, o Direito deve estar sempre atualizado visando a proteção dos cidadãos lesados, aplicando a legislação vigente e concebendo tipos penais específicos para as condutas praticadas na *internet*.

### **1.1 Conceituação de crimes cibernéticos e aspectos gerais sobre sua tipificação penal**

O avanço tecnológico nos meios informáticos é latente e interfere diretamente no modo como as pessoas lidam com a informação e a acessa, as quais buscam através da tecnologia as soluções para seus problemas cotidianos.

---

<sup>16</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 19.

<sup>17</sup> *ibidem*, p. 25.

Concomitantemente e numa velocidade assustadora caminham os crimes praticados através da *internet*, onde criminosos se aproveitam das fragilidades no acesso dos usuários para lhes causar danos, os já popularmente conhecidos crimes cibernéticos.

Para melhor entender o que efetivamente são os crimes cibernéticos, Dario José Kist descreve que o crime é revelado através de dois elementos. O primeiro deles diz respeito ao meio utilizado para a sua prática, e o segundo, o lugar onde são praticadas as condutas. Quanto ao meio utilizado, é assim ensinado por Kist:

Relativamente ao meio, isto é, o instrumento e a forma utilizados para a prática dos atos de que é composto o crime, tem importância o assim chamado “dispositivo informático”. A palavra “dispositivo”, em termos etimológicos, serve para designar um aparato ou aparelho capaz de realizar uma ou várias ações direcionadas a um objetivo; já o termo “informática” nasce da junção das palavras “informação” e “automática”. Decorre que um dispositivo informático é um aparelho capaz de processar de forma automática, dados e informações para um fim determinado, que pode ser qualquer um, inclusive a prática de infração penal. Destaca-se, assim, a relevante função que estes dispositivos exercem nos cibercrimes, ou seja, estes são crimes nos quais os dispositivos informáticos intervêm como meios para cometer o delito, a exemplo de uma ameaça encaminhada à vítima por intermédio de um correio eletrônico, ou como o próprio fim do crime, como o envio de um vírus ao computador da vítima para danificar arquivos, impedir seu funcionamento, capturar informações e dados, inclusive para fins extorsivos.<sup>18</sup>

Quanto ao lugar ou o ambiente em que são desenvolvidas as ações criminosas, trata-se do próprio ciberespaço, ou ainda do próprio ambiente virtual. Já Jesus e Milagre ensinam um conceito jurídico de crime cibernético, sendo este o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação.<sup>19</sup> Os autores ainda ressaltam que o crime cibernético tem deixado de ser exclusivamente um crime-meio, passando a se desenvolver como crime-fim, já que há tipificações de alguns crimes cibernéticos próprios.<sup>20</sup> Verdade é que, como será visto mais adiante, os crimes cibernéticos ainda não possuem tipificação própria e são apurados como meio para a prática de crimes já tipificados no nosso ordenamento jurídico penal.

Delineados os aspectos básicos sobre o entendimento da determinação de um crime cibernético, ponto fundamental para a sua análise é a necessidade de mensurar, numa reflexão preliminar, o quão danoso um crime praticado em ambiente digital será aos usuários da rede quando comparado à prática dos mesmos delitos no ambiente físico.

---

<sup>18</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 62.

<sup>19</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 49.

<sup>20</sup> *ibidem*

Os mecanismos disponíveis em nosso país para a apuração e processamento dos crimes cibernéticos, sejam eles de direito material ou processual, aparentemente não são suficientes para que haja uma efetiva persecução penal, e a resposta do Estado aos criminosos não é capaz de atender a demanda existente, tornando-se branda, quando não nula, passando a sensação de impunidade para aqueles que se aproveitam da tecnologia para a prática delituosa. Além disso, não se pode tratar os crimes comuns e aqueles praticados na *internet* diferenciando-os apenas pelo fato de o criminoso ter usado a rede para o cometimento do delito. A extensão do dano quando o crime é praticado pelo computador ou qualquer outro dispositivo com o acesso à *internet* é, na maioria das vezes, imensurável, pois imaginemos quantos milhares de usuários podem se tornar vítimas de um crime cibernético através de um simples apertar de uma tecla.

Dessa maneira, quando a *internet* é utilizada para a prática de crimes, deveria o criminoso sofrer a reprimenda à altura do potencial do dano que causou ou poderia ter causado, e haveria, portanto, a distinção na apuração entre os crimes praticados no ambiente físico e aqueles praticados no ambiente digital, onde somente uma tipificação adequada e sancionada à altura do potencial do dano poderia então atender aos anseios da sociedade.

No Brasil, diversos são os delitos praticados na *internet*, dentre os quais são exemplos os crimes contra a honra, onde a calúnia, a difamação e a injúria, previstos nos artigos 138, 139 e 140 do CP, respectivamente, são delitos que em razão da facilidade de comunicação por meio das redes sociais e aplicativos de comunicação instantânea, são comumente praticados na rede, cujas penas não ultrapassam 2 (dois) anos de detenção.

A ameaça, previsto no artigo 147 do CP, também é um dos delitos praticados com muita frequência na rede, e o conteúdo ameaçador facilmente alcança a vítima que é ameaçada. Aqui a pena máxima é de 6 (seis) meses de detenção.

A apologia de crime, com previsão no artigo 287 do CP, é constatada através das inúmeras mensagens e imagens de pessoas enaltecendo a prática de crimes que são veiculadas nas redes sociais. Trata-se também de um delito com pena máxima de 6 (seis) meses de detenção.

Há ainda aqueles delitos pelos quais se constata que o agente que os pratica claramente migrou suas atividades criminosas do ambiente físico para o ambiente digital, isto em decorrência do maior alcance que a *internet* proporciona, como é o



caso do furto e do estelionato, previstos nos artigos 155 e 171 do CP, respectivamente. Os criminosos passaram a lançar mão da tecnologia para furtar valores de contas bancárias, bem como para induzir as pessoas à erro para obtenção de vantagens ilícitas.

O potencial de dano aqui não é diferente dos demais delitos praticados na *internet*, sendo absurdamente superior quando comparado aos mesmos delitos praticados no ambiente físico. A pena máxima prevista para o crime de furto é de 4 (quatro) anos e para o crime de estelionato é 5 (cinco) anos.

Ressalta-se que, em virtude da Lei nº 13.964/19, o crime de estelionato somente será apurado mediante representação, salvo quando a vítima for a Administração Pública, criança ou adolescente, pessoa com deficiência mental ou ainda quando for pessoa maior de 70 (setenta) anos de idade ou incapaz.

Ainda em razão das facilidades que a *internet* proporciona para o cometimento de crimes, é bastante comum que criminosos criem perfis falsos para expor à venda medicamentos falsificados ou adulterados, produtos alimentícios e produtos cosméticos sem as devidas especificações legais ou ainda com prazos de validade vencidos, aproveitando-se do alcance da rede para despertar o interesse de um número muito maior de pessoas nestes tipos de produtos. Nestes casos, os delitos cometidos serão os previstos no artigo 273 do CP, com pena máxima de 15 (quinze) anos de reclusão, e ainda os previstos no artigo 7º da Lei nº 8.137/90, com pena máxima de 5 (cinco) anos de detenção.

O tráfico de drogas, previsto no artigo 33 da Lei nº 11.343/06, com pena máxima de 15 (quinze) anos de reclusão, e o comércio ilegal de armas de fogo e tráfico internacional de armas de fogo, previstos nos artigos 17 e 18 da Lei nº 10.826/03, respectivamente, com pena máxima de 8 (oito) anos de reclusão, são delitos comumente praticados na *internet*, porém, os criminosos aqui lançam mão da navegação em áreas da rede que torna quase impossível sua identificação.

O anonimato que essas áreas de navegação proporciona faz com que o tráfico de drogas e o comércio ilegal de armas de fogo sejam delitos praticados livremente na rede. As características destes meios de navegação serão mais bem estudados no tópico 2.2.2, onde serão objetos de estudos a *Deep Web* e a *Dark Web*, áreas da *internet* utilizadas para a prática não somente destes, mas de tantos outros crimes cibernéticos.

Por fim, e sem a pretensão de se esgotar o rol de crimes praticados na *internet*, estão os crimes eleitorais, previstos no Capítulo II da Lei nº 4.737/65. Como é sabido, nos dias atuais a *internet* tornou-se ferramenta indispensável para a realização de campanhas eleitorais, e na mesma velocidade que as campanhas são disseminadas na rede para alcançar um número cada vez maior de eleitores, os crimes eleitorais na *internet* têm se tornado cada vez mais frequentes, onde conteúdos são compartilhados, na sua maioria contemplando notícias falsas, com o principal objetivo de denegrir a imagem daqueles que concorrem aos cargos eletivos.

No rol exemplificativo supra mencionado, o nosso ordenamento jurídico penal em momento algum prevê em suas tipificações a utilização do computador e/ou outros dispositivos com acesso à *internet* como meio para o cometimento dos crimes, sem qualquer previsão legal do agravamento da lesão ocasionada por estarem incluídos nos crimes cibernéticos.

Já no rol de crimes descritos abaixo, as leis penais brasileiras já mencionam na tipificação do crime as expressões “delitos informáticos”, “dispositivos informáticos”, “meio de comunicação de massa ou sistema de informática ou telemática”, “rede mundial de computadores” e “programa de computador”.

São ainda, portanto, crimes cometidos na *internet*, a invasão de dispositivo informático, previsto no artigo 154-A do CP, que foi acrescentado pela Lei nº 12.737/12, cuja pena máxima é de 1 (um) ano de detenção. O delito é configurado pela invasão de um dispositivo informático com a intenção de obter, adulterar ou destruir conteúdos que estejam nele armazenados.

A Lei nº 12.737/12 ficou popularmente conhecida por Lei Carolina Dieckmann, e foi aprovada em meio a uma grande exposição midiática do episódio em que a atriz tornou-se vítima de um criminoso cibernético, que teve acesso a fotos íntimas da atriz ao invadir seu computador pessoal. Aqui é pertinente uma observação: a vítima teve seu computador invadido, suas fotos íntimas foram acessadas e publicadas, expondo sua intimidade para um número inestimável de pessoas, pois essa é uma das principais características da *internet*, ou seja, a abrangência e a facilidade na disseminação de um conteúdo, e o resultado foi uma lei que busca punir o criminoso com uma pena máxima de 1 (um) ano de detenção, o que parece ser branda demais quando comparada ao potencial de dano que o delito alcança.

Outro exemplo de tipificação criminosa que traz na sua descrição a conduta de cometimento na *internet*, é a divulgação de cena de sexo ou pornografia, previsto

no artigo 218-C do CP, que foi acrescido pela Lei nº 13.718/18, cuja pena máxima é de 5 (cinco) anos de reclusão. Trata-se de um delito que comumente é praticado na rede, pois a tipificação da conduta está relacionada com o compartilhamento de cenas de sexo ou nudez sem o consentimento da vítima, como se observa por exemplo nos casos de pornografia de vingança, quando um parceiro ou parceira, descontente com o fim de um relacionamento, torna público a intimidade do casal com o objetivo de vingar-se.

Há ainda os crimes relacionados à pedofilia, previstos nos artigos 240, 241 e 241-A a E da Lei nº 8.069/90, cuja pena máxima é de 8 (oito) anos de reclusão, onde estão tipificadas as condutas de compartilhamento na *internet* de conteúdo com cenas de sexo envolvendo crianças e adolescentes. Aqui se observa a preocupação do legislador em enfrentar a pornografia infantil quando praticada na *internet*, já que o ambiente virtual tornou-se um campo bastante explorado pelos pedófilos.

Por fim, e novamente sem a pretensão de esgotar o estudo dos crimes que já guardam na sua descrição alguma relação expressa ao cometimento de crimes cibernéticos, está a violação de dados, prevista no artigo 10 da Lei nº 9.296/96, com pena máxima de 4 anos de reclusão, e que prevê a conduta criminosa daquele que realiza a interceptação de comunicação de informática ou telemática sem a devida autorização judicial ou com objetivos não autorizados em lei.

Continuando a análise dos crimes cibernéticos, quando estes são devidamente apurados e processados, na sua maioria incidem em tipos penais cujas sanções não ultrapassam dois anos de pena máxima, o que resulta em procedimentos estabelecidos nos Juizados Especiais Criminais. Nestes casos, poderá o autor do crime fazer *jus* aos benefícios dos institutos da Transação Penal e da Suspensão Condicional do Processo, conforme previstos nos artigos 76 e 89 da Lei 9.099/95, respectivamente, o que resulta somente em penas restritivas de direito, e chegando em alguns casos até a extinção da punibilidade do agente. São exemplos os crimes contra a honra, que aqui são considerados crimes de menor potencial ofensivo, e que deixam de considerar todo o potencial de dano que o meio digital pode gerar ao ofendido.

Ressalta-se que com o advento da Lei nº 13.964/19, o chamado pacote anticrime, foi inserido no CPP o artigo 28-A, que prevê a possibilidade de acordo de não persecução penal, desde que respeitados alguns requisitos, dentre eles que o investigado confesse a prática do crime, crime este sem violência ou grave ameaça e

com pena mínima inferior a 4 (quatro) anos, e desde que também sejam respeitadas algumas condições, dentre elas que haja a reparação do dano à vítima. Encontra-se à disposição do criminoso cibernético mais um benefício processual, já que boa parte dos delitos praticados na *internet* se enquadram nos requisitos para sua concessão. Cumprido integralmente o acordo de não persecução penal, será decretada a extinção de punibilidade do agente.

Há ainda a necessidade de que sejam abordadas neste contexto as regras de prescrição (art. 109 do CP) em relação aos crimes cibernéticos, que dadas as dificuldades de se identificar seus autores, tipificar os crimes e vencer todas as fases de um processo judicial, corre-se o risco de que os crimes, quando e se forem levados à julgamento, já estejam prescritos, e mais uma vez a resposta adequada não será alcançada.

Nota-se que a abrangência da lei penal em relação aos crimes cibernéticos ainda é muito reduzida, ocasionando com que a boa parte das condutas cometidas neste ambiente ainda se encontre sem a devida tipificação legal. Ademais, percebe-se que nossos legisladores apenas se mostram sensibilizados à esta matéria quando há casos de grande repercussão nacional, como foi o ocorrido com a atriz Carolina Dieckmann, que teve suas fotos íntimas divulgadas no ambiente virtual sem o seu consentimento, o que gerou na época a promulgação da Lei nº 12.737/12.

Verifica-se, portanto, que o Brasil deve atentar para a necessidade de um projeto legislativo que contemple todo o rol de crimes informáticos, aplicando-se sanções atinentes ao dano e ao potencial de dano que um crime dessa natureza pode causar, atendendo assim aos anseios de uma sociedade mais justa e prestando a devida tutela aos cidadãos e cidadãs.

### **1.2 *Internet versus* criminalidade: superexposição e vulnerabilidade dos usuários**

Como se tem testemunhado ao longo dos últimos anos, as novas tecnologias possibilitaram um novo nível de comunicação, que se promove em tempo real e em escala mundial, sem dificuldades ou qualquer obstáculos aparentes na sua execução. Este contexto criou uma nova realidade, a realidade da sociedade em rede digital, na qual há a superexposição voluntária e involuntária de seus usuários nas redes sociais e mídias em geral.

A propagação e exposição da vida privada e íntima das pessoas se tornou regular e cotidiana, uma vez que divulgam diversos atos de suas vidas no ambiente virtual. Nas palavras de David Lyon, ao referir-se sobre a disponibilização de informações pessoais na teoria da vigilância líquida de Bauman:

Além disso, no que Bauman chama de mundo pós-pan-óptico da modernidade líquida, grande parte das informações pessoais vigorosamente absorvida pelas organizações é, na verdade, disponibilizada por pessoas que usam celulares, compram em shoppings, viajam de férias, divertem-se ou surfam na internet. Passamos nossos cartões, repetimos nossos códigos postais e mostramos nossas identidades de forma rotineira, automática, espontânea.<sup>21</sup>

Ainda nos ensinamentos de Zygmunt Bauman em relação a privacidade: "O privado é público, é algo a ser celebrado e consumido tanto por incontáveis amigos quanto por usuários casuais."<sup>22</sup>

O relacionamento humano passou a ser medido pela tecnologia, e como ensinam Patrícia Martinez Almeida e Vladimir Oliveira Silveira<sup>23</sup>, o compartilhamento de informações pessoais na rede dá-se sem qualquer preocupação com o sigilo destas informações, expondo por consequência a intimidade das pessoas e desencadeando a difusão da vida privada, o que alterou a maneira das pessoas se relacionarem.

Irineu Francisco Barreto Junior ensina sobre essa temática que com a *internet* "Cria-se, no cidadão usuário da rede, um poderoso polo ativo na produção e disseminação de informações e de conteúdo, em escala planetária, relacionados aos mais diversos assuntos (...)."<sup>24</sup> Os benefícios e malefícios dessa nova sociedade são inegáveis. Fato é que essa superexposição da vida privada causa maior vulnerabilidade e cria potenciais vítimas dos mais diversos ilícitos civis e penais no ambiente digital.

Ainda conforme os ensinamentos de Barreto Junior<sup>25</sup>, o que antes estava restrito ao meio privado, agora está num alto patamar de visibilidade e exposição, fruto

<sup>21</sup> BAUMAN, Zygmunt; DAVID, Lyon. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013, p. 20.

<sup>22</sup> *ibidem*, p. 21.

<sup>23</sup> ALMEIDA, Patrícia Martinez; SILVEIRA, Vladimir Oliveira. O direito ao esquecimento e a privacidade. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 619.

<sup>24</sup> BARRETO JUNIOR, Irineu Francisco. Proteção de dados pessoais na *internet*: o marco civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 409.

<sup>25</sup> *ibidem*, p. 414.

da conduta do cidadão digital, que de forma advertida ou não, compartilha com os demais da rede aspectos de sua vida pessoal na rede.

A superexposição das pessoas no ambiente digital parece ocorrer com a finalidade de criar e fortalecer relacionamentos entre os usuários. Entretanto, a busca desse objetivo de forma inadvertida pode levar e já tem levado à vitimização de milhares de pessoas, sendo certo que o dano gerado às pessoas poderá ser imensurável.

As novas tecnologias tornaram real a possibilidade da comunicação em escala planetária, facilitando os interesses dos usuários da rede mundial de computadores. Entretanto, também trouxeram novos riscos e obstáculos à utilização plena das novas ferramentas de comunicação, uma vez que a superexposição voluntária nas mídias e redes sociais, e a obrigatoriedade de fomentar os bancos de dados públicos e privados – para o exercício das atividades por eles disponibilizadas na rede – acabaram por vulnerar diversos direitos dos indivíduos.<sup>26</sup>

A vulnerabilidade das pessoas ao disponibilizar informações privadas no ambiente digital e que venha gerar algum risco aos seus direitos, demanda certamente de um cuidado especial por parte do Estado. Deverão ser adotadas medidas de enfrentamento a esta nova realidade inerente aos novos meios de comunicação, abrangendo inclusive aspectos na esfera criminal, pois, como visto anteriormente, diversas são as condutas lesivas que hoje são praticadas na *internet* e que não encontram nas suas respectivas tipificações o meio da *internet*.

Neste sentido, como ensina Greice Patrícia Fuller, “se verifica a carência criminal, isto é, a necessidade da tutela criminal também no meio ambiente digital, considerado o novo *modus operandi* que indica novos sujeitos ativo e passivo, novas consequências, novos bens a serem tutelados.”<sup>27</sup>

Inquestionável, assim, a necessidade de maiores cuidados dos usuários da rede como forma de proteger sua dignidade, intimidade, imagem, liberdade, segurança e tantos outros direitos que têm sido ameaçados e suplantados por sua superexposição, e também do Poder Público, que deve buscar a adequação das normas à nova realidade social e estabelecer políticas públicas que busquem a

---

<sup>26</sup> ALMEIDA, Patrícia Martinez; SILVEIRA, Vladimir Oliveira. O direito ao esquecimento e a privacidade. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 619.

<sup>27</sup> FULLER, Greice Patrícia. O direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. **VII Congresso brasileiro da sociedade da informação regulação da mídia na sociedade da informação**, 2014, p. 134.

educação e conscientização digital, e que visem minimizar as consequências do que hoje ocorre através da conduta descuidada dos usuários ao navegar na rede.

A *internet* e o acesso às novas possibilidades de se estabelecer a comunicação devem ser utilizados pelos seus usuários de forma consciente e responsável, restringindo-se os excessos de informações que são compartilhadas, e acima de tudo, respeitando-se as informações que são compartilhadas por outros usuários, pois desta forma criar-se-á um ambiente virtual satisfatório para a manutenção das relações interpessoais, sem que se cause danos a outrem e por consequência pratique-se crimes.

### **1.2.1 A responsabilidade ético-social em face do convívio no ambiente virtual**

A responsabilidade é inerente a todos nós. Desde que nascemos, o simples fato de estarmos inseridos na sociedade já nos condiciona a uma série de responsabilidades na medida em que adquirimos a maturidade e nos relacionamos uns com os outros.

Ao longo de nossa existência assumimos a responsabilidade por nós e por nossos semelhantes sem sequer termos essa percepção, pois ela, a responsabilidade, faz parte de nós enquanto seres humanos. Como ensina Evaldo Antonio Kuiava, “o eu é incumbido da responsabilidade, com exclusividade, e a qual não pode humanamente recusar. (...) Essa é a sua identidade inalienável de sujeito. Desse modo, pode afirmar-se que a responsabilidade individua o eu, pois ninguém pode assumir no seu lugar essa condição.”<sup>28</sup>

Nos ensinamentos do filósofo Hans Jonas, que aborda de maneira precisa a existência do Ser e seus deveres:

Somente o Ser vivo, em sua natureza carente e sujeita a riscos – e por isso, em princípio, todos os seres vivos –, pode ser objeto da responsabilidade. Mas essa é apenas a condição necessária, mas não condição suficiente para tal. A marca distintiva do Ser humano, de ser o único capaz de ter responsabilidade, significa igualmente que ele deve tê-la pelos seus semelhantes – eles próprios, potenciais sujeitos de responsabilidade (...)<sup>29</sup>

---

<sup>28</sup> KUIAVA, Evaldo Antonio. A responsabilidade como princípio ético em H. Jonas e E. Levinas: Uma aproximação. **Veritas**, v.51, n.2, Porto Alegre, 2006, p. 59.

<sup>29</sup> JONAS, Hans; tradução do original alemão Luiz Barros Montez, Marijane Lisboa. **O princípio responsabilidade: Ensaio de uma ética para a civilização tecnológica**. Rio de Janeiro: PUC – Rio, 2006, p. 176.

E ainda o mesmo autor, “ser responsável efetivamente por alguém ou por qualquer coisa em certas circunstâncias (mesmo que não reconheça tal responsabilidade) é tão inseparável da existência do homem quanto o fato de que ele seja genericamente capaz de responsabilidade – da mesma maneira que Ihe é inalienável a sua natureza falante (...)”<sup>30</sup>

Hans Jonas estuda a responsabilidade como preceito fundamental frente ao grande avanço tecnológico vivido pela humanidade nas últimas décadas, e nos faz refletir sobre o quão impactante o mau uso das tecnologias pode ser para as gerações futuras. A sociedade capitalista, com seus objetivos de consumo desenfreado impõe riscos ao planeta de modo que não refletir sobre a responsabilidade pode gerar danos irreversíveis num futuro próximo.

A obra de Jonas propõe um novo imperativo relacionado à responsabilidade, e que se adequa ao novo modo como agem as pessoas quando estão diante da tecnologia. É descrito da seguinte maneira: “Aja de modo a que os efeitos da tua ação sejam compatíveis com a permanência de uma autêntica vida humana sobre a Terra”.<sup>31</sup> Diferente da ética tradicional, onde o imperativo de Immanuel Kant voltava-se para o indivíduo, através do ato consigo mesmo, e de forma momentânea, o imperativo proposto por Jonas preocupa-se com os reflexos que as ações presentes causarão ao futuro, de uma forma permanente.

O comportamento das pessoas devem ser revistos, a ponto de repensar a forma como estão lidando com a tecnologia e as prováveis consequências danosas que podem estar ocorrendo (e que certamente estão) não somente ao nosso ambiente, mas também a cada um de nós como detentores de direitos fundamentais que nos são garantidos desde o momento em que nascemos.

O novo imperativo proposto por Jonas é totalmente pertinente na nova ética da civilização tecnológica, pois os impactos das ações irresponsáveis nos novos meios de comunicação são imensamente maiores do que foi no passado, quando não se tinha à disposição todo este aparato. Os efeitos de uma conduta, nos dias de hoje, se prologam no tempo e no espaço, o que não ocorria com os meios de comunicação tradicionais.

---

<sup>30</sup> JONAS, Hans; tradução do original alemão Luiz Barros Montez, Marijane Lisboa. **O princípio responsabilidade: Ensaio de uma ética para a civilização tecnológica**. Rio de Janeiro: PUC – Rio, 2006, p. 176.

<sup>31</sup> *ibidem*, p. 47.



Inseridas neste contexto estão as novas formas de comunicação que são estabelecidas através da *internet* (e já não tão novas assim), uma possibilidade tecnológica que desencadeia uma série de condutas danosas aos seus usuários, e que são causadas por pessoas que, talvez pelo fato de sentirem uma falsa sensação de anonimato, não observam a responsabilidade por seus atos e tampouco observam preceitos éticos minimamente aceitáveis para a boa convivência na rede.

Como ensinam Ângela Kretschmann e Emernon Wendt:

Um dos maiores desafios dessa cibercivilização, ou num plano muito maior, a cibercultura, é conseguir manter íntegros e conscientes a livre-vontade, para que se manifeste no ser humano, considerando que a cada dia logado ele parece sujeitar-se de modo bastante frágil às condicionantes sugestivas do mundo digital, muitas vezes inclusive subliminares das redes sociais.<sup>32</sup>

Os mesmos autores ainda complementam que “é fundamental que se faça a distinção entre os limites que a ética impõe e os limites técnicos. Enquanto a técnica não se preocupa com o estabelecimento de limites, e nem deveria, a ação ética deve refletir sobre os usos da técnica. (...) é o uso que se faz de tudo isso, o “como se usa” que é moral ou imoral.”<sup>33</sup>

Conclui-se, portanto, que o fato de a tecnologia não impor limites ao seu uso não significa dizer que deve-se agir de forma irresponsável, e Kretschmann e Wendt assim ensinam:

Entretanto, muitas pessoas pensam, erroneamente, que aquilo que a tecnologia permite é lícito. Esse é um raciocínio muito simplista, e a cada dia que passa, mais fácil se torna perceber que só pelo fato da tecnologia permitir uma ação, não significa que ela seja lícita. (...) as novas tecnologias, pelo fato de possibilitarem o acesso de um número cada vez maior a um território comum a todos (nem tantos assim, mas isso é discutível em teoria política) também levam as pessoas a pensar automaticamente que aquilo que é possível é consequentemente lícito.<sup>34</sup>

Portanto, não há de se contar com a tecnologia para praticar a moral no lugar das pessoas, e a discussão se dá em torno dos limites que a ética pode e deve impor aos mecanismos que por si só não podem estabelecer esses limites.<sup>35</sup>

O acesso cada vez mais frequente a essas novas formas de comunicação, onde as informações são postadas e compartilhadas instantaneamente e numa abrangência imensurável, acaba gerando uma sensação de poder por parte dos

---

<sup>32</sup> KRETSCHMANN, Ângela; WENDT, Emerson. **Tecnologia da informação & direito**. Porto Alegre: Livraria do advogado, 2018, p. 24.

<sup>33</sup> *ibidem*, p. 25.

<sup>34</sup> *ibidem*, p. 14.

<sup>35</sup> *ibidem*, p. 25.

usuários, ocasionando a não percepção de que a responsabilidade deve ser o preceito básico para o bom convívio neste ambiente.

Hans Jonas ainda ensina que, “por circunstâncias ou por convenção, encontram-se sob meus cuidados o bem-estar, o interesse e o destino de outros, ou seja, o controle que tenho sobre eles. O exercício do poder sem a observação do dever é, então, “irresponsável”, ou seja, representa uma quebra da relação de confiança presente na responsabilidade.”<sup>36</sup>

Quando não há observância de cuidados ao acessar a rede, havendo o exercício do poder sem qualquer preocupação com o dever, aquele que agiu de forma a causar algum dano a outrem deve ser responsabilizado por sua conduta, reparando-o. Jonas assim ensina:

O poder causal é condição da responsabilidade. O agente deve responder por seus atos: ele é responsável por suas consequências e responderá por elas, se for o caso. Em primeira instância, isso deve ser compreendido do ponto de vista legal, não moral. Os danos causados devem ser reparados, ainda que a causa não tenha sido um ato mau e suas consequências não tenham sido nem previstas, nem desejadas.<sup>37</sup>

A consciência do certo e do errado deve ser a regra para que casos de ofensas pessoais, discriminação, discursos de ódio, danos à privacidade e intimidade das pessoas, além de danos à honra, sejam minimizados e deixem de ocorrer com tanta frequência no ambiente digital, mas isso não é o que testemunhamos cotidianamente.

Neste sentido, nos ensinamentos de Evaldo Antonio Kuiava:

Sob o ponto de vista ético o sujeito é responsável quando é capaz de se autodeterminar, quando quer e sabe, isto é, quando tem consciência. O termo consciência refere-se à capacidade de reconhecer que existe algo para além de si. Mas, nesse contexto, ter consciência é ser capaz de reconhecer o bem e o mal, o certo e o errado. Ter consciência ética é ser capaz de escolher e assumir voluntariamente determinadas normas morais, atitudes e posturas éticas diante das mais diversas situações enfrentadas no decorrer da vida pessoal e profissional.<sup>38</sup>

Kuiava ressalta que “a noção de responsabilidade é baseada na noção de escolha livre. Uma ação é livre na medida em que se responde por ela. Em princípio,

---

<sup>36</sup> JONAS, Hans; tradução do original alemão Luiz Barros Montez, Marijane Lisboa. **O princípio responsabilidade: Ensaio de uma ética para a civilização tecnológica**. Rio de Janeiro: PUC – Rio, 2006, p. 168.

<sup>37</sup> *ibidem*, p. 165.

<sup>38</sup> KUIAVA, Evaldo Antonio. A responsabilidade como princípio ético em H. Jonas e E. Levinas: Uma aproximação. **Veritas**, v.51, n.2, Porto Alegre, 2006, p. 57.

se o ser humano é livre, então cabe a ele assumir as consequências dos seus atos. Do contrário não haveria como ser moralmente responsável pelo seu agir.”<sup>39</sup>

As decisões tomadas durante o convívio na rede não podem ocorrer de forma indiscriminada, ao acaso, pois sem a adoção de critérios mínimos de responsabilidade os danos se acumularão e a sociedade só terá a perder com estas espécies de condutas.

Kuiava assim ensina, “cabe a cada um responder, diante de si mesmo e diante dos outros, pelo que faz ou pelo que deveria fazer e não fez. Nesse sentido, a responsabilidade exige fundamentalmente a consciência dos atos praticados, a capacidade de entendimento adequado aos princípios éticos.”<sup>40</sup>

Baseado em suas convicções pessoais, na sua liberdade de agir conforme seu discernimento, o usuário que não é responsável poderá comprometer seu bom convívio na rede, pois nem sempre o que o usuário entende como sendo moralmente correto atenderá as expectativas dos demais, e portanto, o que é correto e justo para si deve ser também para a sociedade e deve atender a ordem moral do coletivo, e não somente do individual.

A ordem moral diz respeito àquilo que se impõe incondicionalmente, para uma consciência. É o conjunto de normas que criamos com o objetivo de controlar nosso comportamento e tem vínculo com as ideias de certo e errado. (...) também é vista como a oposição entre o bem e o mal e entre o dever e a proibição. É uma ordem que tem base no conjunto de nossos deveres, que são as obrigações ou oposições que impomos a nós mesmos. Ela não precisa ser limitada, mas completada, e o que a complementa é a ordem ética.<sup>41</sup>

As ausência de limites que as novas formas de comunicação proporcionam não podem ser exploradas em detrimento aos direitos inerentes a todos nós. Kretschmann e Wendt acrescentam que “isso significa que enquanto alguns direitos representam conquistas políticas importantes do cidadão como o direito à intimidade, à privacidade, à livre associação e à expressão, a esfera ilimitada da ação técnica propicia, por sua vez, uma ameaça a tais exercícios.”<sup>42</sup> E quanto aos desafios enfrentados por esta problemática, os mesmos autores ainda ensinam:

Se tanto se discute acerca da liberdade do ser humano e sua fundamental importância para o pleno desenvolvimento de suas potencialidades criadoras, tudo isso, por outro lado, demandou também a necessidade de se pensar

---

<sup>39</sup> KUIAVA, Evaldo Antonio. A responsabilidade como princípio ético em H. Jonas e E. Levinas: Uma aproximação. **Veritas**, v.51, n.2, Porto Alegre, 2006, p. 57.

<sup>40</sup> *ibidem*, p. 56.

<sup>41</sup> KRETSCHMANN, Ângela; WENDT, Emerson. **Tecnologia da informação & direito**. Porto Alegre: Livraria do advogado, 2018, p. 27.

<sup>42</sup> *ibidem*, p. 22.

novos institutos jurídicos e de se repensar antigos institutos que pudessem dar respostas aos novos problemas. Afinal, assim como a tecnologia trouxe muitas soluções, trouxe também novos problemas, novas soluções e novos desafios.<sup>43</sup>

Entende-se que tais direitos estariam ameaçados pelo próprio avanço tecnológico, principalmente a privacidade e a intimidade. O mau uso da tecnologia que é feita de forma irresponsável torna vulneráveis as informações pessoais dos demais usuários, o que acarreta a lesão de diversos bens jurídicos tutelados, em especial a privacidade, a intimidade e a honra. Aqueles que de forma corriqueira causam essas espécies de lesões, muitas vezes fundamentam suas condutas no exercício do direito à liberdade de expressão, porém, o que será necessário é avaliar se este direito deverá ser exercido com alguns limites.

### 1.2.2 Responsabilidade *versus* liberdade de expressão

O Marco Civil da *Internet*, Lei nº 12.965/14, estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, e confere papel de destaque ao direito à liberdade de expressão. Conforme prevê em seu artigo 2º, a liberdade de expressão é fundamento para a disciplina do uso da *internet* no Brasil. No artigo 3º, surge como princípio disciplinador da mesma matéria, e ainda no artigo 8º, é condição para o pleno exercício do direito de acesso à rede. Nos ensinamentos de Carlos Affonso Pereira de Souza:

No que diz respeito aos danos causados na Internet e a consequente responsabilização de seus agentes, a liberdade de expressão desempenha ainda dois relevantes papéis. O caput do artigo 19, que estabelece a regra para responsabilização dos provedores de aplicações de Internet, é iniciado com a expressão “com o intuito de assegurar a **liberdade de expressão e impedir a censura**”. Com relação aos danos causados aos direitos autorais na Internet, o Marco Civil, no parágrafo segundo do mesmo artigo 19, afirma que a aplicação do regime de responsabilização por ele determinado depende de previsão legal específica. Embora essa redação desloque o tratamento do tema para outro processo de alteração legislativa, é importante destacar que, segundo o dispositivo mencionado, essa nova legislação deverá “respeitar a **liberdade de expressão** e demais garantias previstas no art. 5º da Constituição Federal”. (grifo do autor)<sup>44</sup>

---

<sup>43</sup> KRETSCHMANN, Ângela; WENDT, Emerson. **Tecnologia da informação & direito**. Porto Alegre: Livraria do advogado, 2018, p. 14.

<sup>44</sup> SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 377.

Anderson Schreiber ensina que “a *internet* é usualmente vista como uma aliada da liberdade de expressão. Sua capacidade de “amplificar” o alcance das manifestações individuais é frequentemente apontada como um estímulo à livre circulação de ideias.”<sup>45</sup>

Para tanto, o exercício da liberdade de expressão será livre, não sendo admitido o anonimato, ocasião, portanto, em que as manifestações anônimas deixarão de ser protegidas, conforme o artigo 5º, inciso IV da Constituição Federal. Ainda nos ensinamentos de Schreiber:

O problema não se resume, contudo, a uma ausência de efetividade concreta da propalada liberdade de expressão no universo virtual, mas atinge a própria essência da liberdade de expressão, na medida em que as novas formas de comunicação na internet, se aparentemente incentivam o exercício dessa liberdade, em cada vez maior medida também a oprimem. Não há aqui um paradoxo. O extremismo e o radicalismo – fruto do caráter individualista que vem se ampliando nesses novos ambientes comunicativos – descambam, não raro, para agressões verbais, rotulações estigmatizantes e discursos de ódio que se espalham pela rede.<sup>46</sup>

A liberdade de expressão, portanto, vem sendo utilizada como pretexto para inúmeras manifestações lesivas no ambiente digital, mais especificamente nos meios social e político. Manuel Castells, em sua reflexão quanto ao exercício do direito à liberdade de expressão, assim ensina:

E como num mundo de redes digitais em que todos podem se expressar não há outra regra além da autonomia e da liberdade de expressão, os controles e censuras tradicionais se desativam, as mensagens de todo tipo formam uma onda bravia e multiforme, os *bots* multiplicam e difundem imagens e frases lapidares aos milhares, e o mundo da pós-verdade, do qual a mídia tradicional acaba participando, transforma a incerteza na única verdade confiável: a minha, a de cada um.<sup>47</sup>

O que se observa é a disseminação de conteúdos ofensivos, discriminatórios, e muitas vezes criminosos, e neste sentido, revestidos de total irresponsabilidade, sem qualquer cuidado com as condutas lesivas que afrontam os bens tutelados das outras pessoas. Como ensina Schreiber:

A percepção do impacto devastador que a veiculação de material sobre uma determinada pessoa na internet pode produzir em sua vida real é apenas uma das muitas circunstâncias que confirmam a necessidade de aplicação das

---

<sup>45</sup> SCHREIBER, Anderson. Marco civil da *internet*: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 278.

<sup>46</sup> *ibidem*, p. 281.

<sup>47</sup> CASTELLS, Manuel; tradução Joana Angélica d’Avila Melo. **Ruptura: a crise da democracia liberal**. Rio de Janeiro: Zahar, 2018, p. 28.

regras jurídicas ao mundo virtual. A internet não pode representar uma bolha de irresponsabilidade dentro da vida em sociedade.<sup>48</sup>

O que corrobora para ampliar as lesões provenientes de condutas irresponsáveis no meio ambiente digital é o excesso de compartilhamento de informações pessoais na rede, que de certo modo torna a vida privada do usuário em pública. O que os demais usuários não observam é que isso não os autoriza a se manifestarem como bem entenderem, de forma irresponsável, como se o detentor daquelas informações existisse apenas no mundo virtual e não no físico. Zygmunt Bauman, em suas sábias palavras, ensina que “privado é público, é algo a ser celebrado e consumido tanto por incontáveis “amigos” quanto por “usuários” casuais.”<sup>49</sup> E ainda conclui:

Nos dias de hoje, o que nos assusta não é tanto a possibilidade de traição ou violação da privacidade, mas o oposto, o fechamento das saídas. A área da privacidade transforma-se num lugar de encarceramento, sendo o dono do espaço privado condenado e sentenciado a padecer expiando os próprios erros; forçado a uma condição marcada pela ausência de ouvintes ávidos por extrair e remover os segredos que se ocultam por trás das trincheiras da privacidade, por exibi-los publicamente e torná-los propriedade comum de todos, que todos desejam compartilhar.<sup>50</sup>

O exercício da liberdade de expressão certamente deve ser exercido na sua plenitude, sem violações ou qualquer tipo de censura, porém devemos refletir quando o exercício se torna abusivo, momento em que afronta outros direitos fundamentais de igual hierarquia, como a privacidade, a intimidade e a honra. Neste caso o exercício da liberdade de expressão deve encontrar limites. Os excessos devem ser sanados para que violações não ocorram, e na possibilidade de ocorrerem, serem os usuários responsabilizados pela conduta lesiva. A conduta ilícita, seja ela na esfera penal ou na esfera não penal, deve ser enfrentada através dos meios legislativos e processuais hoje disponíveis, e o seu causador deve ser responsabilizado por seus atos.

---

<sup>48</sup> SCHREIBER, Anderson. Marco civil da *internet*: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 283.

<sup>49</sup> BAUMAN, Zygmunt; DAVID, Lyon; tradução Carlos Alberto Medeiros. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013, p. 21.

<sup>50</sup> *ibidem*, p. 34.

### 1.3 Ofensividade *on-line* e responsabilização penal

A especificidades e características da criminalidade no ambiente virtual, assim como ocorre nos crimes praticados no ambiente físico, poderão variar de acordo com os aspectos sociais, culturais, econômicos, e até políticos de uma nação. Como apresentado nos tópicos anteriores, há a propensão de a *internet* ser utilizada por seus usuários sem a mínima preocupação em preservar sua intimidade, tornando-os vulneráveis e suscetíveis a tornarem-se vítimas não somente de crimes contra a honra, mas também, por exemplo, de crimes contra o patrimônio.

Não bastasse o uso da *internet* de forma irresponsável, chama-se a atenção para o fato da existência daqueles que fundamentam o uso no exercício da liberdade de expressão, o que não justifica extrapolar suas condutas e ferirem outros direitos de igual relevância. Nos ensinamentos de Fuller quanto aos limites que devem ser observados ao direito à liberdade de expressão:

De toda forma, é imprescindível que os direitos de expressão, informação e comunicação encontrem limites na dignidade do outro e não que se reduza à prática do alheamento humano. Para além disso, é de suma importância que se afirme que tais direitos, especialmente, instrumentalizados pela mídia encontram limites e não podem gerar condutas imponderáveis e antissociais sob o falacioso pensamento de ser o mundo virtual sinônimo de mundo anônimo. Clara é a necessidade da consciência de que do outro lado da comunicação não existe um simples personagem imaginário, sem vida privada e sem honra, mas uma pessoa humana, considerando-se que o mundo virtual não é um mundo meramente cerebrino no qual os atos, as opiniões, as declarações, as exposições feitas ao outro se colocam à margem do controle da legalidade, legitimidade e ético-moral.<sup>51</sup>

Aliada à navegação por muitas vezes irresponsável de uma parcela dos usuários e o excesso do exercício do direito à liberdade de expressão, está a sensação de impunidade por parte dos cibercriminosos, os quais contam com a certeza de que jamais serão identificados e punidos, perpetuando suas atividades ilícitas e aperfeiçoando cada vez mais seu *modus operandi*. Há ainda de se mencionar o fato de que quando identificados, por uma ausência de tipificações específicas quanto ao uso da *internet* como meio para a prática delituosa, os autores, quando punidos, não receberão sanções à altura dos atos praticados.

Além das peculiaridades ligadas ao aspecto sociocultural dos usuários, as próprias características dos crimes cibernéticos os tornam crimes mais difíceis de

---

<sup>51</sup> FULLER, Greice Patrícia. O Direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. **VII Congresso brasileiro da sociedade da informação regulação da mídia na sociedade da informação**, 2014, p. 136.

serem solucionados. A plurilocalidade, a multiplicidade de vítimas, a instantaneidade e velocidade de abrangência, além da possibilidade de serem praticados de qualquer lugar do mundo, bastando para isso o acesso à *internet*, todos esse fatores somados, potencializam os danos causados e não raramente desencadeiam consequências desastrosas às vítimas. Como será estudado mais adiante, o compartilhamento indiscriminado de conteúdos na *internet* é uma característica bastante presente no ambiente virtual, e vem tornando-se um dos principais desafios no enfrentamento das lesões causadas às pessoas, incorrendo inclusive e principalmente em diversos ilícitos penais, o que promove em não raras vezes até a morte social de uma pessoa.

### 1.3.1 A morte social como extensão do dano

A divulgação e o compartilhamento de uma informação de forma irresponsável poderá gerar danos irreversíveis a uma pessoa. A velocidade e a abrangência que uma notícia pode atingir na rede, aliadas ao poder lesivo da informação disseminada poderá causar, a morte social do indivíduo. A depender da gravidade da notícia que foi veiculada, a vítima não encontrará mais espaço em seu meio social, profissional, e eventualmente, por que não dizer, até familiar, e passará a experimentar a difícil sensação de ter morrido para a sociedade.

A vítima da lesão sofrerá as consequências da conduta criminosa, podendo ser afrontada, diminuída, excluída, etc., e a depender do conteúdo da publicação e seu alcance, sofrer até as consequências da morte social. É como se a pessoa tivesse que nascer novamente, adquirindo outra identidade, mudando de domicílio, iniciando do zero uma vida que foi devastada com a veiculação anterior de notícia lesiva.

Isso quando não ocasiona sua morte real, como no caso da dona de casa que foi brutalmente assassinada na cidade do Guarujá, no litoral paulista, por ter sido relacionada a uma notícia falsa veiculada na *internet*, que tratava de uma suposta mulher que sequestrava crianças para a realização de magia negra naquela localidade.<sup>52</sup>

Os criadores e compartilhadores de conteúdo devem, portanto, atentar-se para o fato de que uma publicação realizada de forma irresponsável poderá causar

---

<sup>52</sup> FOLHA DE SÃO PAULO / UOL. **Veja o passo a passo da notícia falsa que acabou em tragédia no Guarujá.** Disponível em: <https://www1.folha.uol.com.br/cotidiano/2018/09/veja-o-passo-a-passo-da-noticia-falsa-que-acabou-em-tragedia-em-guaruja.shtml>. Acesso em: 05 ago. 2019.



danos muitas vezes irreversíveis, e, além disso, o direito penal deveria ponderar a proporcionalidade do dano quando uma informação lesiva é veiculada na rede, atentando para a elaboração de leis que venham contemplar este tipo de conduta, além é claro, de estabelecer programas educativos de conscientização dos usuários da rede para essa problemática atual.

Como verificado, o compartilhamento de conteúdos ilícitos através da *internet* é uma das ações mais comuns entre os usuários da rede, e dada a velocidade e abrangência na veiculação, alcança um número inestimável de pessoas. O recurso do compartilhamento torna vulnerável aquele usuário que, ao submeter-se a uma superexposição de sua vida privada, permite que sejam estabelecidas circunstâncias para a prática de diversos crimes no ambiente digital.

Além disso, não se pode respaldar o compartilhamento de um conteúdo ilícito no exercício do direito à liberdade de expressão, pois este encontra limites em outros direitos tão relevantes quanto, como a honra, a privacidade e a intimidade. Destaca-se que os danos causados por um conteúdo disponibilizado e compartilhado na rede poderão se tornar irreversíveis, ocasionando até a morte social daquele que teve seus bens jurídicos afetados.

A responsabilidade do usuário que compartilha na rede um conteúdo ilícito é, portanto, um desafio a ser superado, principalmente pela ausência de uma legislação que contemple referida conduta. A atuação mais efetiva do poder legislativo, aliada a adoção de políticas públicas de conscientização de melhor uso e convívio na *internet* certamente irá minimizar os danos que a criação e o compartilhamento de um conteúdo ilícito pode causar, permitindo ainda que os usuários que acessam a rede com o único objetivo de causar lesão a outrem possam ser devidamente punidos por seus atos.

O compartilhamento indiscriminado de conteúdo através da *internet* tem gerado ainda outra grande inquietação por parte da sociedade, o surgimento de inúmeras notícias falsas, as já popularmente conhecidas *fake news*. Há uma preocupação bastante pertinente quanto à divulgação deste tipo de conteúdo, já que, pela abrangência que a notícia pode tomar, aliada ao número de usuários da rede, poderá gerar consequências extremamente danosas à sociedade.

As *fake news* são mundialmente consideradas como um fenômeno social que merece especial atenção das autoridades, além dos provedores e usuários de *internet*, especialmente quanto as consequências sociais, econômicas e políticas que

essa espécie de conteúdo pode acarretar. O surgimento da veiculação de uma notícia falsa se dá principalmente pela ausência de cuidados mínimos de segurança que deveriam ser adotados pelo usuário compartilhador, que ao receber um determinado conteúdo não checa a veracidade e a idoneidade da informação, restringindo sua conduta apenas no compartilhamento, obtendo para si o bônus pela divulgação da notícia, sem a mínima preocupação com o ônus. Nos ensinamentos de Clarissa Piterman Gross a respeito da conceituação de *fake news*:

As *Fake News* seriam, portanto, um tipo novo de conteúdo produzido a partir de uma intencionalidade apenas viabilizada pelo modelo de produção, disseminação e consumo de conteúdo *online*. Trata-se do conteúdo mentiroso, ou seja, intencionalmente falso, fabricado com o objetivo de explorar as circunstâncias do universo *online* (o anonimato, a rapidez de disseminação da informação, a fragmentação das fontes de informação e da atenção dos usuários da internet, e o apelo às emoções e ao sensacionalismo) (...)<sup>53</sup>

Além do conceito apresentado, Greice Patrícia Fuller e Irineu Francisco Barreto Junior ensinam alguns aspectos fundamentais para o melhor entendimento das *fake news* quando inseridas no contexto da sociedade da informação e utilizadas como estratégias para criar a comunicação da desinformação.

Fake News não são apenas notícias falsas ou simples mentiras. São componentes de estratégias comunicacionais de desinformação bastante sofisticadas e que envolvem desde a produção de conteúdo deliberadamente fraudulento, falso, distorcido, enviesado ideologicamente, além da distribuição e impulsionamento dessas mensagens pela Internet, redes sociais, plataformas de vídeo e ferramentas de comunicação em tempo real. Inauguram uma nova era de desinformação política em decorrência das funcionalidades desenvolvidas pelas Tecnologias de Comunicação e Informação, da hiperconectividade inaugurada com a invenção dos smartphones e dos novos padrões de sociabilidade estabelecidos pela Internet.<sup>54</sup>

Aquele que cria um conteúdo mentiroso, o faz com a intenção clara de afrontar e causar danos aos bens jurídicos daquele que é objeto da notícia, e há a certeza de que seu objetivo será alcançado, dada a facilidade e rapidez com que um conteúdo é compartilhado na rede. Carlos Eduardo Nicoletti Camillo ensina que a relação entre a mentira e a vontade de prejudicar alcança um poder lesivo inimaginável quando

---

<sup>53</sup> GROSS, Clarissa Piterman. *Fakenews e democracia: discutindo o status normativo do falso e a liberdade de expressão*. In: RAIS, Diogo (Org.). **Fakenews – a conexão entre a desinformação e o direito**. São Paulo: Revista dos Tribunais, 2018, p. 157.

<sup>54</sup> FULLER, Greice Patrícia; BARRETO JUNIOR, Irineu Francisco. Desinformação e covid-19 no Brasil: desafios e limites do enquadramento penal da disseminação de notícias falsas. In: LIMA, Fernando Rister de Souza; MARTINI, Sandra Regina; SMANIO, Gianpaolo Poggio; WALDMAN, Ricardo Libel (coords.). **Covid-19 e os impactos no direito: mercado, Estado, trabalho, família, contratos e cidadania**. São Paulo: Almedina, 2020, p. 40.

disseminado nas redes sociais, onde alguns influenciadores digitais possuem até milhões de seguidores na rede.<sup>55</sup>

O conceito de *fake news* expõe a necessidade de que sua criação e veiculação implique na existência de dolo, porém a conduta do compartilhamento da notícia, conforme será estudado em tópico posterior, poderá, a depender da previsão culposa do crime, ter suas implicações penais.

Há ainda uma outra questão relevante envolvendo as *fake news*, que é o fato de que o compartilhamento estaria baseado na plenitude do exercício do direito da liberdade de expressão, porém, o que os defensores desta linha de pensamento esquecem é que há outros direitos fundamentais tão importantes quanto e que merecem ser tutelados de igual maneira, como a honra, a privacidade, a intimidade, e a imagem. Flavia Piva Almeida Leite e Samantha Ribeiro Meyer-Pflug contribuem para a ideia de que o direito à liberdade de expressão não pode ser visto como absoluto, e assim nos ensina:

A garantia da liberdade de expressão pressupõe um sistema estruturado e organizado de liberdade em harmonia com os demais valores protegidos pelo ordenamento jurídico. A proteção à liberdade não é absoluta. A expressão de ideias é passível de restrições, na exata medida em que se devem respeitar outros valores albergados pela Constituição da República, com repercussão na legislação infraconstitucional.<sup>56</sup>

Portanto, o direito à liberdade de expressão deverá existir, porém não servirá de justificativa para afrontar e causar danos a outros direitos fundamentais também relevantes, fazendo-se necessário a proteção desses direitos. Ressalta-se que, numa sociedade onde as pessoas estão imersas em todo o tipo de informação e são, na sua maioria, muito bem informadas, o conteúdo com veracidade duvidosa e que certamente colocará em risco bens jurídicos de terceiros, não poderá e nem deverá passar despercebido aos olhares e discernimento daqueles que dedicam horas de seu dia ao acesso das redes sociais.

Outro ponto bastante relevante numa sociedade totalmente inserida na informação digital e que demanda maiores cuidados por parte do Estado em dar maior proteção aos cidadãos e cidadãs é a ausência de uma tipificação penal que abarque

---

<sup>55</sup> CAMILLO, Carlos Eduardo Nicoletti. O fenômeno do fakenews e a sua repercussão na responsabilidade civil no sistema jurídico brasileiro. In: RAIS, Diogo (Org.). **Fakenews – a conexão entre a desinformação e o direito**. São Paulo: Revista dos Tribunais, 2018, p. 225.

<sup>56</sup> MEYER-PFLUG, Samantha Ribeiro; LEITE, Flavia Piva Almeida. A liberdade de expressão e o direito à privacidade no marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2104)**. São Paulo: Quartier Latin, 2015, p. 435.

as notícias falsas. As *fake news* não são tipificadas em nosso ordenamento jurídico penal, de modo que a responsabilização pela criação e compartilhamento deste tipo de conteúdo se dará através dos tipos penais que protegem o bem jurídico afetado, como por exemplo, nos crimes contra a honra.

Observa-se que dada a relevância do tema e a forma como são disseminadas as notícias falsas, atentando-se ainda para seu potencial de dano e a instantaneidade de sua veiculação na rede, há a necessidade de o poder legislativo dedicar-se com maior atenção a este tema tão preocupante e que vem causando danos irreparáveis a um grande número de pessoas.

Segundo reportagem do jornalista Pedro Grigori<sup>57</sup>, tramitam no Congresso Nacional aproximadamente 20 projetos de lei que pretendem criminalizar a divulgação e o compartilhamento das notícias falsas. São exemplos dos referidos projetos de lei o PL nº 9.838/2018, que tipifica criminalmente a conduta de quem oferece, publica, distribui, difunde notícia ou informação que sabe ser falsa em meios eletrônicos ou impressos, e também o PL nº 9.884/2018, que tipifica como crime a divulgação de informação falsa.

Assim, aquele que compartilha na *internet* conteúdo falso deverá ser responsabilizado por sua conduta, e mesmo que ainda não exista uma norma expressa que descreva o compartilhamento de *fake news* como uma prática delituosa, deve-se atentar para a análise das condutas já previstas como crimes e que poderão ser tipificados nos conteúdos das *fake news*.

### 1.3.2 Responsabilização penal por compartilhamento de conteúdo

A grande maioria dos tipos penais relacionados aos crimes praticados em ambiente digital, como já mencionado, em momento algum prevê em suas tipificações a utilização do computador e/ou outros dispositivos com acesso à *internet*, tampouco prevê o compartilhamento dos conteúdos ilícitos como uma infração penal. Um ponto que vem sendo bastante debatido na sociedade da informação é a responsabilidade penal daquele que compartilha um conteúdo criminoso.

---

<sup>57</sup> GRIGORI, Pedro. **Pública: agência de jornalismo investigativo**. 20 projetos de lei no Congresso pretendem criminalizar fake news. Disponível em: <https://apublica.org/2018/05/20-projetos-de-lei-no-congresso-pretendem-criminalizar-fake-news/> . Acesso em: 05 de ago. 2019.

A análise aqui é a do alcance da responsabilidade penal para além dos sujeitos que criaram e postaram o conteúdo na *internet*, abrangendo também a conduta daqueles que o compartilha em suas redes, questão esta relevante à sociedade da informação no que diz respeito ao comportamento dos usuários, que muitas vezes, sem adotar qualquer critério de segurança e verificação da idoneidade do conteúdo, acaba compartilhando-o de forma indiscriminada.

A grande maioria dos crimes cibernéticos previstos em nosso ordenamento jurídico penal não prevê o compartilhamento de conteúdos ilícitos como uma infração penal. O que há é a previsão de condutas delitivas cometidas através da *internet*, porém sem a previsão do compartilhamento como uma conduta criminosa, como por exemplo a discriminação (art. 20 da Lei nº 7.716/89), a pirataria (art. 12 da Lei nº 9.609/98,) e violação de dados (art. 10 da Lei nº 9.296/96).

Já no rol de crimes descritos a seguir, nossas leis penais trazem na sua tipificação, além das expressões específicas dos crimes cibernéticos, como “delitos informáticos”, “dispositivos informáticos”, “meio de comunicação de massa ou sistema de informática ou telemática”, “rede mundial de computadores” e “programa de computador”, também a previsão expressa das condutas de compartilhamento, sendo eles:

- Invasão de dispositivo informático, art. 154-A do Código Penal: *Invasão de dispositivo informático alheio (...), e seu parágrafo 1º : Na mesma pena incorre quem produz, oferece, **distribui**, vende ou **difunde** dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (grifo nosso)*

- Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia, art. 218-C do Código Penal: ***Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -**, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia. (grifo nosso)*

- Pedofilia, art. 241-A da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente: ***Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática***

ou *telemático*, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. (grifo nosso)

Constata-se, portanto, que em nosso ordenamento jurídico penal a previsão da conduta de compartilhamento como crime é prevista de forma pontual em apenas alguns tipos penais, sendo que para os demais crimes praticados no ambiente virtual ainda não há a referida previsão.

Ressalta-se que o conteúdo poderá ter sido criado por alguém que não necessariamente será identificado e/ou punido, porém, aquele que compartilha o conteúdo ilícito (a se analisar sua conduta quanto ao dolo ou culpa, e a depender da previsão legal da punição aos crimes culposos) deverá ser responsabilizado por sua conduta. A seguir alguns apontamentos quanto ao dolo e a culpa no compartilhamento de conteúdos ilícitos.

Crime doloso, conforme prevê o art. 18 do CP, é aquele cujo agente quis o resultado ou assumiu o risco de produzi-lo. Assim, o dolo baseia-se, sobretudo, na vontade do agente em produzir um resultado ou ainda no risco de produzi-lo após ter a consciência de que poderá provocá-lo, o que gera neste último os casos de dolo eventual. Ao analisar o conceito de dolo e aplicá-lo ao compartilhamento de um conteúdo ilícito na *internet*, o usuário estará sujeito às sanções penais desde que tenha a vontade de produzir o resultado ou se assumir o risco de produzi-lo.

Nesses dias em que o compartilhamento de conteúdos através das redes sociais parece ser uma necessidade vital para o convívio social em rede, o principal objetivo dos usuários parece ser a obtenção de notoriedade através do maior número de "*likes*", ocorrendo nitidamente uma disputa para se saber quem chegará ao final do dia na liderança de popularidade de seus conteúdos frente aos seus concorrentes da rede. Diante deste fato, os usuários devem redobrar suas atenções para não se deixarem envolver pelas tentações digitais e serem responsabilizados pelos danos que causarem pelo compartilhamento de conteúdos ilícitos. Necessário ressaltar que, como muitos assim o fazem, o compartilhamento com a finalidade de, por exemplo, realizar uma brincadeira ou de simplesmente exercer a liberdade de expressão no ambiente virtual, poderá levar aos compartilhadores serem responsabilizados criminalmente.

Por outro lado, quando o compartilhamento de um conteúdo ilícito causar um dano, e este dano decorrer de culpa do usuário que o postou, ele apenas será responsabilizado se a modalidade culposa estiver prevista no tipo penal, ficando

isento de toda e qualquer responsabilidade criminal se não existir referida previsão legal. Neste sentido será necessário analisar a aplicabilidade das modalidades de culpa na conduta do agente, ou seja, se o usuário deixou de observar o dever de cuidado, agindo com imprudência, negligência ou imperícia, e ainda avaliar se a conduta prevê a modalidade culposa como ilícito penal.

Somente com a soma destes condicionantes é que poderá o usuário compartilhador ser responsabilizado criminalmente, pois caso contrário, estaremos diante de uma conduta atípica, mesmo que o conteúdo postado tenha causado algum dano a outrem. Tal fato decorre da previsão do parágrafo único do art. 18 do CP, que descreve que salvo os casos expressos em lei, ninguém pode ser punido por fato previsto como crime, senão quando o pratica dolosamente. Desta forma, a conduta culposa praticada por um usuário e que incida em um crime cibernético será responsabilizada apenas na hipótese de que esta esteja expressamente tipificada.

O compartilhamento indiscriminado de conteúdos em busca de popularidade na rede tem gerado inúmeros casos de danos no ambiente digital, principalmente em casos que venham atingir a honra, a privacidade e intimidade das pessoas, e que as coloca frente a uma situação injuriosa, caluniosa ou difamatória. Porém, nada impede que o compartilhamento de um conteúdo acabe por gerar outro tipos de danos, cuja previsão legal se dará fora dos crimes contra a honra e que atingirá outros bens jurídicos tutelados, repercutindo numa sanção ainda mais grave.

Dentre o rol de crimes praticados na *internet*, alguns trazem expressamente a previsão da modalidade culposa, o que permite analisar a responsabilidade pelo compartilhamento de um conteúdo ilícito nesses casos. A seguir alguns exemplos de descrições de tipos penais que contemplam a modalidade culposa.

Nos crimes de falsificação, corrupção, adulteração ou alteração de substância ou produtos alimentícios, com previsão no art. 272 do Código Penal, há a previsão da conduta de **expor à venda**, prevista no parágrafo 1º-A, existindo ainda a modalidade culposa prevista no parágrafo 2º do mesmo artigo. Portanto, nos crimes contra a saúde pública previstos no Código Penal, há a previsão da modalidade culposa, e especificamente quanto ao compartilhamento, ao analisar o núcleo do tipo, a expressão “expõe à venda” se enquadra perfeitamente quanto ao sujeito que compartilha a oferta, por exemplo, de um medicamento falsificado em suas redes sociais ou qualquer outro meio no ambiente virtual.

Necessário enfatizar que a regra é o dolo, e a modalidade culposa deverá ser analisada no caso concreto para verificar se houve a incidência de uma das modalidades da culpa no compartilhamento (imprudência, negligência ou imperícia).

Nos crimes contra a relação de consumo, com previsão no art. 7º da Lei nº 8.137/90, também há a conduta de **expor à venda**, prevista nos incisos II, III, e IX, existindo também a modalidade culposa, prevista no parágrafo único. Da mesma maneira que a análise dos crimes contra a saúde pública, aqui nos crimes contra a relação de consumo há também a previsão da modalidade culposa, cabendo aqui a mesma interpretação quanto a expressão “expor à venda”, onde a responsabilidade penal pelo compartilhamento pode ocorrer quando na análise do caso concreto estiver presente uma das modalidades da culpa já elencadas e o usuário oferecer à venda, por exemplo, produtos alimentícios impróprios para o consumo em razão da data de validade expirada.

O que se verifica é que o compartilhamento de um conteúdo ilícito não fica restrito apenas aos casos de crimes praticados contra a honra, abrangendo um rol de crimes ainda maior, abarcando ainda a tutela de outros bens jurídicos, havendo a necessidade de os conteúdos recebidos serem submetidos à mínimos critérios de segurança para a verificação de sua licitude, o que minimizará eventuais responsabilizações criminais pelo compartilhamento de conteúdo na modalidade culposa. Além disso, a verificação prévia de conteúdo adequa o uso da *internet* através da conscientização por parte dos usuários, levando-a a um patamar onde ocorra uma incidência de danos em número cada vez menor.



## **2 – Criminalidade na Sociedade da Informação: desafios no enfrentamento e a busca pela efetividade estatal**

O segundo capítulo da pesquisa abará alguns aspectos relacionados aos crimes cibernéticos que aqui são colocados como entraves no seu enfrentamento, gerando uma oportunidade de reflexão quanto às melhorias que ainda poderão ser buscadas na persecução penal e sua efetividade. A determinação da jurisdição e da competência será um tópico estudado com ênfase na característica da plurilocalidade do crime cibernético, demandando atenção especial na correta aplicação da lei processual penal.

A apuração e colheita de provas no ambiente virtual também será objeto de estudo, demonstrando que o crime que deixava vestígios físicos, agora ocupa um ambiente onde as provas tornam-se mais suscetíveis ao perecimento. O ambiente da *Deep Web* e a *Dark Web* também farão parte do objeto de estudo deste capítulo, onde será mais bem esclarecido como os criminosos fazem uso deste meio de navegação para tentar burlar a investigação e manterem-se impunes.

### **2.1 Estabelecimento da jurisdição e da competência nos crimes cibernéticos**

Uma das questões mais desafiadoras quanto a persecução penal dos crimes cibernéticos é a correta determinação da jurisdição e da competência, isso em virtude dessas espécies de crimes possuírem a peculiar característica da plurilocalidade, podendo atingir ainda a transnacionalidade, características estas que os diferem dos demais crimes praticados no ambiente físico. Diante desta problemática na aplicação da lei processual penal, como deverá ser fixada a jurisdição e a competência nos crimes cibernéticos diante das regras que atualmente dispomos? Como se dará a interpretação e a aplicação nos seus respectivos processos penais? Além disso, qual é o posicionamento jurisprudencial em relação a matéria?

Preliminarmente, quanto ao conceito de jurisdição, no entendimento doutrinário, é o poder que o Estado detém de aplicar o direito ao caso concreto, resguardando a ordem jurídica e a autoridade legal. Ao poder judiciário é dada a função da aplicação das normas por meio de um processo, que é pautada em diversos

princípios (investidura, juiz natural, devido processo legal, indeclinabilidade jurisdicional, etc.), objetivando sempre a solução de uma demanda.

Como o Estado tem o dever jurisdicional, ou seja, a obrigação de solucionar conflitos, não poderá eximir-se de prestar a devida tutela quando for acionado (princípio da indeclinabilidade jurisdicional), conforme descrito no art. 5º, inciso XXXV da Constituição Federal, prevendo que a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça de direito. Dario José Kist ainda ensina que: “(...) a jurisdição, no campo penal, é exercida para a aplicação da lei penal, leia-se, comprovada, no bojo de um processo, a ocorrência de infração penal e respectiva autoria, permite-se impor ao agente do crime a sanção prevista em lei.”<sup>58</sup>

Quanto a aplicação das leis processuais penais no tempo, conforme previsto no art. 2º do Código de Processo Penal, serão aplicadas de imediato, desde sua vigência e respeitando os atos realizados sob o amparo da lei anterior. Admite-se ainda a retroatividade da lei processual desde que não envolvam questões de direito material, o que poderia em tese prejudicar o acusado. Já no que se refere às leis processuais no espaço, serão aplicadas a todo território nacional (princípio da territorialidade), conforme prevê o art. 1º do CPP: O processo penal reger-se-á, em todo o território brasileiro, por este Código (...), excetuando-se os casos de extraterritorialidade previstos no art. 7º do Código Penal, onde estão previstos os casos em que a lei extrapolará os limites territoriais para responsabilizar determinadas pessoas e condutas praticadas fora do território nacional.

Ainda quanto ao princípio da territorialidade, o que se busca é assegurar a soberania nacional quanto à aplicação da lei processual penal aos casos ocorridos em seu território. Diante da adoção do princípio da territorialidade em matéria processual penal, há um grande desafio para a correta fixação da jurisdição nos crimes cibernéticos. O desafio se encontra no fato de que este tipo de crime não encontra barreiras físicas ou limites territoriais para sua execução e consumação, sendo a plurilocalidade uma característica que impõe aos órgãos de persecução penal e investigação cuidados extras nos modos de abordagem.

Neste sentido, nos ensinamentos de Alesandro Golçaves Barreto e Beatriz Silveira Brasil, os cibercrimes na grande maioria das vezes se caracterizam por serem plurilocais, quando vítima e agente estão em locais distintos, ou, ainda, quando a

---

<sup>58</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 90.

execução do delito se inicia em um lugar e a consumação ocorre em outro, mas no mesmo país.<sup>59</sup>

Passando-se ao conceito de competência, trata-se da delimitação da jurisdição, ou seja, o espaço dentro do qual pode determinada autoridade judiciária aplicar o direito aos litígios que lhe forem apresentados, compondo-o.<sup>60</sup> Dentro do conceito de competência, extrai-se, portanto, o entendimento de que determinado juiz será declarado competente para processar e julgar uma matéria (prestar a jurisdição), de acordo com cada caso concreto, que será determinada obedecendo-se alguns critérios estabelecido em lei.

Para a determinação de qual juiz será competente para determinado conflito, o Código de Processo Penal estabelece três critérios em seu art. 69. São eles: o critério *ratione loci* (em razão do lugar), previsto nos incisos I e II; o critério *ratione materiae* (em razão da matéria), previsto no inciso III; e o critério *ratione personae* (em razão da pessoa), previsto no inciso VII.

O primeiro critério a ser levado em consideração para a fixação da competência é o lugar onde ocorreu o crime (*ratione loci*), sendo essa a regra. O CPP, em seu art. 70, traz a previsão da fixação da competência em razão do local da infração, ou pelo local do último ato de execução no caso de tentativa. O Código Penal, em seu art. 6º, complementa trazendo a previsão de que local da infração é aquele da ação/omissão, ou ainda onde produziu ou deveria produzir o resultado, tratando-se aqui da denominada teoria da ubiquidade.

Caso o crime seja consumado fora do território nacional, a competência será determinada pelo lugar onde tiver sido praticado o último ato de execução no Brasil. Nos casos em que ocorrerem conflitos para a fixação da competência pelo fato de envolverem duas ou mais jurisdições, ou se o crime for continuado ou permanente, ela será determinada pela prevenção (o juiz que proferir qualquer decisão relacionada ao fato criminoso, mesmo que anterior ao oferecimento da denúncia, será o competente para julgá-lo), nos termos do art. 71 do CPP.

Ainda em relação à *ratione loci*, quando for desconhecido o local da infração, aplica-se subsidiariamente a fixação da competência pelo domicílio ou residência do acusado, conforme inciso II do artigo 69 e artigo 72, ambos do CPP.

---

<sup>59</sup> BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do marco civil da internet**. Rio de Janeiro: Brasport, 2016, p. 25.

<sup>60</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 213.

Em algumas situações a lei deixa de estabelecer a competência pelo lugar da infração (regra), e irá fixá-la em razão da matéria (*ratione materiae*), como é o caso dos crimes dolosos contra a vida, que será julgado pelo Tribunal do Júri, bem como os crimes eleitorais e os crimes militares, os quais serão julgados respectivamente pelas Justiça Eleitoral e Justiça Militar. Como o objetivo da pesquisa é a aplicação da lei processual penal aos crimes cibernéticos, desnecessário aprofundar o estudo à fixação da competência em razão da matéria.

Da mesma maneira que a fixação da competência em razão da matéria, a lei também prevê casos especiais, onde pessoas com prerrogativa de função, ao cometerem crimes, serão julgadas por órgão específicos. O julgamento dos processos criminais por prerrogativa de função está previsto na Constituição Federal, a qual estabelece que o Supremo Tribunal Federal, o Superior Tribunal de Justiça, os Tribunais Regionais Federais e os Tribunais de Justiça processarão e julgarão por crimes comuns e de responsabilidade, como exemplos, o Presidente da República, os Ministros de Estado, os Governadores de Estado, os Prefeitos, os Juízes Federais e Juízes Estaduais, etc.

Importante ressaltar que em maio de 2018, o Plenário do Supremo Tribunal Federal decidiu que o foro por prerrogativa de função conferido aos Deputados Federais e Senadores se aplica apenas a crimes cometidos no exercício do cargo e em razão das funções a ele relacionado, restringindo-se, portanto, a aplicabilidade das prerrogativas de função previstas na Constituição Federal. De acordo com a decisão, os parlamentares federais que cometerem crimes mesmo no exercício do cargo, mas que não tenham qualquer relação com as funções que exercem, terão sua competência fixada pelos critérios gerais do Código de Processo Penal.<sup>61</sup>

Como é verificado, muitos são os desafios encontrados quando o assunto é o enfrentamento aos crimes cibernéticos. Alesandro Gonçalves Barreto, Emerson Wendt e Guilherme Caselli ensinam que, no dia a dia da atividade de persecução penal exercida pelas polícias judiciárias, é comum verificar o aperfeiçoamento de técnicas e meios de execução das atividades ilícitas por parte dos criminosos que a todo momento procuram meios para se esquivar da atuação policial.<sup>62</sup>

---

<sup>61</sup> BRASIL. Supremo Tribunal Federal. **STF conclui julgamento e restringe prerrogativa de função a parlamentares federais.** Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=377332>. Acesso em: 07 out. 2019.

<sup>62</sup> BARRETO, Alesandro Golçaves; WENDT, Emerson; CASELLI, Guilherme. **Investigação digital em fontes abertas.** Rio de Janeiro: Brasport, 2017, p. 208.

Damásio de Jesus e José Antonio Milagre complementam que a tecnologia da informação integrou o mundo em uma grande teia, onde todos têm acesso a tudo, pouco importando o local físico em que realmente esteja armazenado tal conteúdo. Ocorre que, para a Justiça, o local físico da prática de um ato digital tem relevância para determinar a competência judiciária.<sup>63</sup>

Como se já não bastasse a ausência de tipificação penal para diversas condutas ilícitas que já estão sendo praticadas no ambiente virtual, além de toda a dificuldade na identificação e colheita de um conjunto probatório satisfatório para a identificação e punição dos autores neste tipo de delito (assunto que será melhor detalhado no item 2.2 deste trabalho), há ainda toda a problemática vivida pelos órgãos jurisdicionais acerca da fixação da competência nos crimes praticados no ambiente virtual.

### 2.1.1 Extraterritorialidade e transnacionalidade

O crime cibernético possui a característica que o difere dos demais crimes, que é a extraterritorialidade, podendo abranger inclusive, a transnacionalidade, atingindo dois, três, e por muitas vezes, diversos países. Kist ensina que, de fato, os cibercrimes não se fixam às linhas que separam um país de outro; na verdade, desprezam-nas totalmente, em dois sentidos: as fronteiras físicas não representam entraves para sua prática, e também não servem para (de)limitar geograficamente os efeitos e consequências desses crimes.<sup>64</sup>

Por se tratar de delitos que, ao ocuparem o espaço virtual, desencadeiam diversos resultados, em diversos locais diferentes, além de atingirem múltiplas vítimas, a determinação jurisdicional para os crimes cibernéticos tem se mostrado uma tarefa bastante complexa e que ainda é bastante divergente.

Com efeito, é uma criminalidade que cria situações jurídicas plurilocalizadas, são infrações que têm caráter difuso ou transnacional e capacidade para afetar, simultânea e independentemente do local da prática do fato, as ordens jurídicas de vários Estados, contendo, portanto, elementos de extraneidade. Desta plurilocalização de condutas penalmente ilícitas nasce uma gama de situações problemáticas, dentre as quais podem ser citadas as questões que dizem respeito à aplicação da lei no espaço e a consequente definição de jurisdição estatal com competência para conhecer e julgar tais infrações. Nessas condições, a cibercriminalidade tem capacidade ou, pelo menos,

---

<sup>63</sup> JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 179.

<sup>64</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 78.

potencialidade de causar movimentação no assim chamado Direito Penal Internacional (...)<sup>65</sup>

O legislação penal brasileira, conforme já mencionado no que se referiu à parte conceitual desta pesquisa, traz a previsão de que a regra para a fixação da competência será o local onde se deu o resultado do delito, que será determinado pelo local da ação/omissão ou onde produziu ou deveria ter produzido o resultado. Neste sentido, KIST nos ensina:

Como se sabe, o estudo do lugar do crime é instrumental para definir a jurisdição, nacional ou internacional, com a competência para a ação penal; os critérios usualmente manejados para o efeito são a ação/omissão e a consumação do crime, perquirindo-se do lugar em que esses eventos se manifestaram e, com a resposta, identificar a jurisdição competente. É nesse campo que os cibercrimes promovem significativos problemas jurídicos, pois uma de suas características, já apontada, situa-se no fato de poderem ser praticados a distância, leia-se, os efeitos da atividade criminosa poderão ser observados em local diverso, muitas vezes distante, isto é, em país diverso daquele da situação física do agente e do lugar onde ele praticou os atos executórios; como já referido, os cibercrimes produzem situações jurídicas plurilocalizadas, projetando dúvidas para o campo da definição da jurisdição penal competente e criando possíveis conflitos a esse propósito.<sup>66</sup>

Outro aspecto relevante quanto a fixação da competência nos crimes cibernéticos, quando esses tiverem o caráter transnacional, é o fato da conduta em discussão ser ou não tipificada como crime em todos os países em que foi gerado algum resultado, ou até mesmo, caso positiva a resposta, se determinado país entenderá ser plausível a colaboração no sentido de fornecer informações para a obtenção do conjunto probatório sob o pretexto da proteção de sua soberania.

Essa possível fragmentação geográfica nos cibercrimes provoca problemas tanto em nível substantivo, pois, na falta de uma uniformização na seleção de condutas típicas, pode ocorrer que um desses países afetados a conduta não se revista de caráter criminoso, o que, ao menos em tese, afasta o interesse deste país em persegui-la, assim como pode refletir-se em ausência de vontade em colaborar com a coleta de prova nele eventualmente existente.<sup>67</sup>

E continua ensinando que:

É que tanto a lei penal como as leis processuais penais foram e são pensadas para atuarem no interior dos limites geográficos do país que as edita, e o ciberespaço veio, de forma contundente, a desafiar essa limitação; e ainda não há critérios internacionalmente consensuados para a resolução dos grandes problemas que a cibercriminalidade apresenta, dentre os quais os efeitos da territorialidade das leis.<sup>68</sup>

<sup>65</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 76.

<sup>66</sup> *ibidem*, p. 81.

<sup>67</sup> *ibidem*, p. 82.

<sup>68</sup> *ibidem*, p. 83.

Portanto, faz-se necessário a colaboração recíproca dos países envolvidos para o enfrentamento aos crimes cibernéticos, pois somente assim todos encontrarão as soluções que atendam seus plenos interesses.

Ainda em continuidade ao estudo da transnacionalidade, que aqui significa dizer o envolvimento de mais de um país como vítimas de crimes cibernéticos, outro ponto bastante intrigante, e que a doutrina vem dedicando bastante atenção, é a possibilidade do autor/autores sofrerem mais de uma punição por um mesmo fato, ou, em casos opostos, deixarem de sofrer qualquer tipo de sanção, permanecendo impunes. Quanto a essas duas possibilidades, Celso Antonio Pacheco Fiorillo e Christiany Pegorari Conte ensinam que desta maneira, há a necessidade de solução da questão da territorialidade da *internet*, tendo em vista que muitos delitos podem ser cometidos através da rede e, sem uma regulamentação clara e eficaz, correremos o risco de que um delito possa ser julgado em toda e qualquer parte do mundo ou, ainda, que não haja punição.<sup>69</sup>

No caso da impunidade, basta que os países vitimados pelo crime não tenham em seu ordenamento jurídico penal a tipificação daquela conduta como um fato criminoso. Exemplo que muito bem exemplificou essa problemática bastante nos trouxe Spenser Toth Sydow, em sua Dissertação de Mestrado:

Outra característica do cibercrime é que a conduta em questão pode não ser ilegal (Brenner 2001). Em maio de 2000, o vírus “Eu te amo” atravessou o mundo em duas horas e causou bilhões de dólares em danos em mais de 20 países. Ele foi rapidamente rastreado com origem nas Filipinas, onde agentes do FBI e autoridades legais identificaram um suspeito. Mas como a lei filipina não criminalizava a disseminação de vírus, levou-se dias para se conseguir um mandado de busca no apartamento do suspeito, dando-lhe tempo para destruir as evidências. E ainda havia o problema processual (...) tendo-se em vista que disseminação de vírus não era crime local, o suspeito não poderia ser extraditado para ser processado nos Estados Unidos, onde o fato era crime (...) ninguém nunca foi processado pela disseminação em tela.<sup>70</sup>

Contrapondo-se à impunidade do agente, não se pode afastar a possibilidade de que dois ou mais países, no exercício de sua soberania, pleitearem o direito de apurar e sancionar o responsável por um crime cibernético, podendo ocorrer, neste caso, o *bis in idem*. Neste sentido, KIST ensina que: (...) não é juridicamente possível excluir a jurisdição penal de algum dos países tocados pelo cibercrime praticado a

---

<sup>69</sup> FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2. ed., São Paulo: Saraiva, 2016, p. 206.

<sup>70</sup> SYDOW, Spenser Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/pt-br.php>, p. 95. Acesso em: 07 out. 2019.

distância ou em trânsito. E a mais singela das consequências que daí decorre é que o mesmo fato pode ser objeto da persecução penal em mais de um Estado soberano.<sup>71</sup>

Em sentido contrário, os Tratados e Convenções Internacionais que versam sobre direitos fundamentais e direitos humanos não admitem a possibilidade de uma pessoa sofrer mais de uma sanção pelo mesmo fato, e, portanto, àqueles países que assinaram e ratificaram os referidos tratados, essa possibilidade deverá ser afastada. Sobre os fundamentos do *ne bis in idem*, sustenta-se que eles residem na necessidade de segurança jurídica, e ele funciona como uma limitação ao poder punitivo estatal, concretizando a ideia de que a cada indivíduo será aplicada a sanção correspondente e suficiente para seus atos.<sup>72</sup>

As possibilidades aqui elencadas quanto a impunidade e o *bis in idem* são adicionadas àquelas já conhecidas problemáticas que envolvem o estabelecimento da competência nos crimes cibernéticos, tornando o assunto ainda mais complexo.

### 2.1.2 Competência em território nacional

Com o objetivo de se estabelecer critérios para a fixação da competência em território nacional, a legislação brasileira adotou a teoria da ubiquidade, onde, segundo o artigo 6º do CP, local do crime é aquele em que ocorreu a ação ou omissão, ou ainda onde produziu ou deveria produzir o resultado. Acrescenta-se ainda as hipóteses de aplicação extraterritorial da lei penal brasileira, prevista no artigo 7º do mesmo ordenamento jurídico. Quanto a teoria da ubiquidade, Kist assim ensina:

(...) é de uso geral, para a definição do local do crime, a teoria da ubiquidade, que considera como tal o lugar da ação/omissão e o do resultado e, no caso da tentativa, é onde o resultado deveria ter sido observado. E, com esse parâmetro, pode-se concluir que lugar do crime, para efeito da identificação da ordem jurídica aplicável para o seu conhecimento e julgamento, é qualquer um daqueles pelos quais a atividade criminosa transitou – serão lugar ou da ação, ou do resultado.<sup>73</sup>

Bastante apropriada é a conclusão apontada pelo mesmo autor quando trata das possibilidades em que o crime cibernético terá sua competência fixada em território nacional, descrevendo quatro situações em o que o lugar do crime será em território nacional:

---

<sup>71</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 91.

<sup>72</sup> *ibidem*, p. 95.

<sup>73</sup> *ibidem*, p. 85.



(...) conclui-se haver pelo menos quatro situações em que o Brasil é o lugar do crime, a ensejar a aplicação da lei penal brasileira e o poder de praticar atos tendentes à punição do agente: a) quando a ação/omissão ocorreu nele, mesmo que o resultado tenha ocorrido fora dele; b) quando a ação/omissão foi praticada fora do país, mas nele ocorreu o resultado; c) quando a ação/omissão foi praticado fora do Brasil, mas neste o crime teria se consumado, não fosse a circunstância alheia à vontade do agente que impediu a consumação (é o caso de tentativa, em que o resultado “deveria produzir-se” no Brasil), d) nos casos e condições de extraterritorialidade da lei penal brasileira previstos no art. 7º do Código Penal.<sup>74</sup>

Na prática, o que se verifica é que mesmo nos crimes cibernéticos praticados em território nacional, ainda há conflitos quanto a fixação de competência, e a análise do caso concreto é o que tem prevalecido para sua determinação, variando sua fixação de acordo com a incidência do tipo penal.

Abaixo segue algumas decisões jurisprudenciais que ilustrarão a referida questão:

CONFLITO NEGATIVO DE COMPETÊNCIA. QUEIXA-CRIME. CALÚNIA PRATICADA, EM TESE, POR JORNALISTA. CARTA PUBLICADA EM BLOG. LEI DE IMPRENSA. NORMA NÃO RECEPCIONADA PELA CONSTITUIÇÃO DE 1988. ART. 70 DO CÓDIGO DE PROCESSO PENAL. COMPETÊNCIA DO JUÍZO SUSCITADO. 1. Não recepcionada a Lei n. 5.250/1967 pela nova ordem constitucional (ADPF n. 130/DF), às causas decorrentes das relações de imprensa devem ser aplicadas as normas da legislação comum, inclusive, quanto à competência, o disposto no art. 70 do Código de Processo Penal. 2. O crime de calúnia (art. 138, caput, do Código Penal) consuma-se no momento em que os fatos "veiculados chegam ao conhecimento de terceiros" (CC n. 107.088/DF, Relatora Ministra Maria Thereza de Assis Moura, DJe de 4/6/2010). 3. Tratando-se de queixa-crime que imputa a prática do crime de calúnia em razão da divulgação de carta em blog, na internet, o foro para processamento e julgamento da ação é o do lugar de onde partiu a publicação do texto tido por calunioso. 4. In casu, como o blog em questão está hospedado em servidor de internet sediado na cidade de São Paulo, é do Juízo da 13ª Vara Criminal dessa comarca a competência para atuar no feito. 5. Conflito conhecido para declarar competente o suscitado. (CONFLITO DE COMPETÊNCIA Nº 97.201 - RJ (2008/0150084-3). RELATOR : MINISTRO CELSO LIMONGI (DESEMBARGADOR CONVOCADO DO TJ/SP). DATA DE JULGAMENTO: 13 de abril de 2011).<sup>75</sup>

Aqui entendeu o relator que no crime de calúnia, a consumação ocorre quando os fatos veiculados chegam ao conhecimento de terceiros, e, neste caso, a competência deveria ser o local de onde partiu a publicação do conteúdo calunioso, ou seja, o local onde estava sediado o servidor de *internet* que hospedava o blog utilizado para a divulgação (determinou-se a competência pelo local da ação).

CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSUAL PENAL. FURTO MEDIANTE FRAUDE. TRANSFERÊNCIA BANCÁRIA VIA

<sup>74</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 86.

<sup>75</sup> BRASIL. Superior Tribunal de Justiça. **Conflito de competência nº 97.372 – SP**. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/19134047/conflito-de-competencia-cc-97372-sp-2008-0147300-8/inteiro-teor-19134048?ref=juris-tabs>. Acesso em: 07 out. 2019.

INTERNET SEM O CONSENTIMENTO DA VÍTIMA. CONSUMAÇÃO NO LOCAL DA AGÊNCIA ONDE O CORRENTISTA POSSUI A CONTA FRAUDADA. COMPETÊNCIA DO JUÍZO SUSCITADO. 1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal - CP. 2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal - CPP; no caso, na Comarca de Barueri/SP. Conflito de competência conhecido para declarar competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP, o suscitado. (CONFLITO DE COMPETÊNCIA Nº 145.576 - MA (2016/0055604-1) RELATOR: MINISTRO JOEL ILAN PACIORNIK. Data de Julgamento 13 de abril de 2016).<sup>76</sup>

Já aqui, o relator entendeu que o crime de furto mediante fraude por meio da *internet*, mais especificamente transferência de valores fraudulenta, consuma-se no local onde está estabelecida a agência bancária onde a vítima possui a conta, fixando a competência neste local (determinou-se a competência pelo local do resultado).

CONFLITO DE COMPETÊNCIA. CRIME DE AMEAÇA PRATICADO POR WHATSAPP E FACEBOOK. ÂMBITO DE APLICAÇÃO DA LEI MARIA DA PENHA. DELITO FORMAL. CONSUMAÇÃO NO LOCAL ONDE A VÍTIMA CONHECE DAS AMEAÇAS. CONFLITO DE COMPETÊNCIA CONHECIDO. DECLARADA A COMPETÊNCIA DO JUÍZO SUSCITADO. 1. O crime de natureza formal, tal qual o tipo do art. 147 do Código Penal, se consuma no momento em que a vítima toma conhecimento da ameaça. 2. Segundo o art. 70, primeira parte, do Código de Processo Penal, "A competência será, de regra, determinada pelo lugar em que se consumar a infração". 3. No caso, a vítima tomou conhecimento das ameaças, proferidas via Whatsapp e pela rede social Facebook, na Comarca de Naviraí, por meio do seu celular, local de consumação do delito e de onde requereu medidas protetivas. 4. Independentemente do local em que praticadas as condutas de ameaça e da existência de fato anterior ocorrido na Comarca de Curitiba, deve-se compreender a medida protetiva como tutela inibitória que prestigia a sua finalidade de prevenção de riscos para a mulher, frente à possibilidade de violência doméstica e familiar. 5. Conflito conhecido para declarar a competência do Juízo da 1ª Vara Criminal da Comarca de Naviraí/MS, ora suscitado. CONFLITO DE COMPETÊNCIA Nº 156.284 - PR (2018/0008775-5) RELATOR : MINISTRO RIBEIRO DANTAS DATA DE JULGAMENTO 28 de fevereiro de 2018).<sup>77</sup>

Neste caso, o relator entendeu que no crime de ameaça por meio da *internet* (*whatsapp* e *facebook*) a consumação se dá no local onde a vítima tomou conhecimento do conteúdo ameaçador, independente de onde tenha partido (determinou-se a competência pelo local do resultado).

<sup>76</sup> BRASIL. Superior Tribunal de Justiça. **Conflito de competência nº 145.576 – MA**. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/339952309/conflito-de-competencia-cc-145576-ma-2016-0055604-1/inteiro-teor-339952319>. Acesso em: 07 out. 2019.

<sup>77</sup> BRASIL. Superior Tribunal de Justiça. **Conflito de competência nº 156.284 – PR**. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/552870809/conflito-de-competencia-cc-156284-pr-2018-0008775-5/inteiro-teor-552870818?ref=juris-tabs>. Acesso em: 07 out. 2019.

Sobre a teoria da ubiquidade, Barreto e Brasil ensinam que assim, em se tratando do local do crime virtual uma ficção jurídica, é imprescindível a interpretação da legislação processual pautada na Teoria da Ubiquidade, para se considerar, caso a caso, o lugar do crime onde ocorreu a ação ou o resultado, visando a busca da verdade real e a escorreita aplicação da lei penal.<sup>78</sup> Nota-se que a fixação da competência nos crimes cibernéticos, mesmo nos casos em que esteja ausente a característica de transnacionalidade, ainda requer um estudo mais aprofundado de cada caso concreto, e muitas vezes ainda divergindo opiniões.

Diante de tudo o que foi exposto até aqui, inevitável o seguinte questionamento: Como deverão ser resolvidos os conflitos de jurisdição e competência?

Buscando essa resposta, nos ensinamentos de KIST:

É intuitivo que o lugar para onde se projetam as respostas a essa questão situa-se, de modo especial, no campo da determinação da competência para investigar e julgar tais crimes. Mas, ainda que se consiga formular essas respostas, deve-se adiantar que esse é o campo da maior e mais intensa indefinição, tanto na doutrina como na jurisprudência, e também no âmbito das relações internacionais.<sup>79</sup>

A doutrina e a jurisprudência ainda não estabeleceram um posicionamento pacífico acerca dessa matéria, e não será suficiente, pelo que foi estudado, que a fixação da competência seja determinada pelo local do crime, pois, como visto, por se tratar de infrações penais de características plurilocais e transnacionais, poderá haver mais de um processo para a apuração de um determinado fato, ou nenhum, a depender da tipificação penal dos países envolvidos.

Kist esclarece que a escolha do local do resultado é justificada no fato de, em regra, encontrarem-se nele as provas da infração penal e, com isso, facilitar a investigação e o processo; na cibercriminalidade, contudo, as provas poderão estar em lugar totalmente alheio tanto ao da conduta quanto ao local do resultado (...).<sup>80</sup>

E ainda aprofundando o conhecimento quanto à dificuldade em se estabelecer a jurisdição adequada ao enfrentamento dos crimes cibernéticos, Kist ensina que:

A síntese de tudo é que, no estado atual da matéria, não existe solução consensuada sobre a identificação da jurisdição penal competente para os casos em que o cibercrime manifesta-se a distância ou em trânsito. Além disso, é previsível que não será tarefa fácil essa definição, a demandar muito estudo, pesquisa, análise e negociação entre os países. Mas, ao mesmo

---

<sup>78</sup> BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do marco civil da internet**. Rio de Janeiro: Brasport, 2016, p. 28.

<sup>79</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 84.

<sup>80</sup> *ibidem*, p. 102.

tempo, é um caminho que necessariamente deverá ser trilhado para enfrentar essa que é uma das muitas causas da impunidade no campo da cibercriminalidade. E, para além de definir a jurisdição penal prevalente, também os mecanismos de cooperação internacional para a coleta de prova devem ser aperfeiçoados para os casos em que o processo ocorre em país diverso daquele em que as evidências se encontram.<sup>81</sup>

Quanto aos aspectos pertinentes à cooperação entre países, no ano de 2001 foi firmado pelo Conselho da Europa o tratado internacional que visa estabelecer uma regulamentação comum e ações conjuntas que possibilitem a cooperação internacional para persecução penal em casos de crimes cometidos na *internet*, a chamada Convenção do Cibercrime ou Convenção de Budapeste, e que será mais bem estudada no Capítulo 3 deste trabalho, mais especificamente no tópico 3.3.

Como ensinam Damásio de Jesus e José Antonio Milagre, é bastante comum que os agentes busquem praticar delitos por meio de sistemas hospedados no exterior, e nesses casos a investigação no Brasil necessitará da cooperação de provedores de serviços e de conexão que estarão estabelecidos fora do país, o que não será uma tarefa fácil, considerando que parte das empresas costumam alegar que não estão sujeitas à jurisdição brasileira.<sup>82</sup>

O Brasil, até a data de 14 de outubro de 2020 não havia aderido à Convenção, e o senso comum é que essa será uma importante ferramenta para o enfrentamento dos crimes cibernéticos, e que trará inúmeros benefícios à redução da criminalidade cibernética em nosso país.

## **2.2 Ambiente virtual e prova: desafios na colheita do conjunto probatório satisfatório**

Nas atividades de investigação policial dos crimes cibernéticos é bastante comum as autoridades se depararem com inúmeros desafios em virtude do aperfeiçoamento de técnicas e meios de execução adotados pelos criminosos, sempre na tentativa permanente de se esquivar da persecução penal. Neste sentido, muitos são os desafios enfrentados na busca da identificação e punição dos autores dos crimes cibernéticos.

---

<sup>81</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 102.

<sup>82</sup> JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 179.

Não bastasse a plurilocalidade e transnacionalidade dos crimes, a multiplicidade de agentes ativos, bem como o número imensurável de vítimas que podem ser afetadas por uma única conduta, a busca pela apuração de um conjunto probatório satisfatório é, sem dúvida, um dos grandes obstáculos enfrentados pelos agentes públicos no enfrentamento à cibercriminalidade.

A ausência de barreiras físicas no ambiente digital, o anonimato dos criminosos, que é obtido através de recursos técnicos que dificultam a identificação dos autores, aliadas à velocidade da evolução tecnológica, constituem obstáculos na investigação criminal no enfrentamento aos crimes cibernéticos, e fazem deste um dos maiores desafios da atualidade.

A obtenção da prova no ambiente digital é tarefa extremamente complexa, e em virtude das características dos crimes cibernéticos, faz com que a investigação criminal nesta área seja tarefa onde o conhecimento técnico específico e altamente qualificado seja fundamental para o êxito das investigações. A migração da criminalidade do ambiente físico para o ambiente virtual criou um fator extra de complexidade na apuração de um crime cibernético, pois as provas, que antes deixavam vestígios palpáveis, hoje precisam ser buscadas distante dos olhos de quem investiga. Assim ensinam Guilherme Berti de Campos Guidi e Francisco Rezek quanto as dificuldades da persecução penal em ambiente virtual:

A delinquência, em um cenário natural, pode ser tratada na forma geralmente adotada nos últimos séculos pelos Estados democráticos, com julgamento e sanção, diante da apuração dos fatos: materialidade e autoria contidos em determinado território, em determinada circunscrição, em um processo linear, concentrado. De certo modo, as mesmas mudanças operadas nas vidas dos usuários são as sentidas na persecução penal: os limites não são mais territoriais ou físicos, mas virtuais.<sup>83</sup>

Kist ainda complementa ensinando que as evidências de natureza digital apresentam características que as tornam peculiares, nomeadamente se comparadas com aquelas que não têm essa natureza, o que impacta na forma de abordá-las, identificá-las e recolhê-las, estabelecendo-se, por conta disso, claras diferenças na investigação criminal que as tenha por objeto.<sup>84</sup>

Em tese, a identificação de um criminoso virtual deveria ser uma tarefa relativamente fácil, pois ao se conectar na *internet*, qualquer um de nós o faz através

---

<sup>83</sup> GUIDI, Guilherme Berti de Campos; REZEK Francisco. Crimes na *internet* e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 278.

<sup>84</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 115.

de um provedor de acesso, que atribuirá um endereço de IP para esta finalidade, atribuindo informações de conexão durante nossa permanência *online*. Essas informações ficam registradas no provedor, e o usuário ao interagir com os serviços na *internet*, deixa uma espécie de rastro digital, que poderá ser seguido posteriormente para a colheita de provas em caso de cometimento de crime. Nos ensinamentos de Jesus e Milagre:

Deste modo, diante do uso criminoso de um serviço, ainda que de forma anônima, como, por exemplo, na criação de uma comunidade, grupo, ou página destinada à pornografia infantil, sabe-se que o provedor de serviços (pago ou gratuito) registra os dados de acesso à aplicação (em alguns casos, até mesmo as atividades realizadas – embora muitos afirmem que não), porém tais registros só são fornecidos com ordem judicial. Obtendo-se os dados de acesso às aplicações daquele que utilizou o serviço para más finalidades, pode-se, através do IP (*Internet Protocol*), que será fornecido, descobrir qual o Provedor de Acesso associado ao IP (caso o usuário não tenha mascarado a conexão), e, com isto, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, dentre outros) da pessoa responsável pela conta de Internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa.<sup>85</sup>

Os autores ressaltam que a identificação do usuário será possível somente caso a conexão não seja burlada, fato que, na velocidade que a tecnologia avança e os inúmeros artifícios que os criminosos utilizam para não serem identificados, como por exemplo a utilização da navegação na *internet* na *Deep web* e *Dark web*<sup>86</sup>, tornam ainda mais árdua a tarefa da identificação e recolhimento da prova digital. Neste sentido, nos ensinamentos de Fiorillo e Conte:

Uma das maiores problemáticas no tocante à punição dos crimes praticados em meio ambiente digital diz respeito às provas sobre a materialidade delitiva e aos indícios de autoria que fornecem a mínimo viabilidade (*justa causa*) à propositura de uma ação penal. Nesse sentido, os óbices encontrados ao longo da investigação criminal bem como do eventual processo penal, vão desde a identificação de um possível autor e sua localização (identificar o IP – protocolo de Internet – que identifica a máquina de onde partiu a conduta – o que não significa, necessariamente, identificar o sujeito criminoso), passando pela validade e licitude das provas colhidas e, por fim, as dificuldades de rastreamento das condutas quando praticadas através da denominada *deep web*.<sup>87</sup>

Os crimes cibernéticos, quando comparados aos crimes que deixam vestígios físicos, encontram problemática voltada a não dispersão das evidências, e que por se encontrarem em ambiente digital, tornam-se mais suscetíveis ao perecimento.

---

<sup>85</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 170.

<sup>86</sup> *Deep web* e *Dark web* serão tratadas neste estudo em tópico específico mais adiante.

<sup>87</sup> FIORILLO, Celso Antonio Pacheco, CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2. ed. São Paulo: Saraiva, 2016, p. 215.

Referida circunstância demanda um cuidado especial na sua abordagem, e que, diferentemente dos crimes praticados fora do ambiente digital, por mais desafiador que ainda seja coletar provas no ambiente físico, e por mais que se preze pela preservação do local do crime (o que muitas vezes deixa de ocorrer), as evidências permanecem fisicamente presentes. Complementando o raciocínio, Kist ensina que:

Como referido, trata-se de uma realidade própria, em tudo distinta daquela em que os crimes deixam evidências externas, físicas e, portanto, perceptíveis aos sentidos, e que, naturalmente, demanda métodos diferenciados de investigação e com ela compatíveis. Embora as evidências digitais existam e também tenham uma realidade, esta é no geral imperceptível a quem não detém conhecimentos específicos em matéria informática, razão pela qual é imperativo que a investigação criminal em ambiente digital seja levada a cabo por especialistas em Ciência Forense Digital. A estes caberá, manejando ferramentas por meio de procedimentos forenses adequados, recuperar arquivos eliminados, encontrar registros da conta utilizada pelo agente do crime e, em geral, reconstruir a atividade por este desenvolvida para chegar ao resultado ilícito. Cuidados especiais deverá ter para não contaminar ou mesmo perder, com sua atividade, as evidências encontradas, assim como observar o marco legal incidente, nomeadamente para não afetar, indevidamente, direitos fundamentais envolvidos na investigação (intimidade, privacidade, sigilo da comunicação, etc.).<sup>88</sup>

Diante dos desafios enfrentados na busca de um conjunto probatório robusto e satisfatório para que o titular da ação penal possa iniciar a persecução processual, é fundamental que os agentes públicos (mais especificamente os policiais que atuam nas delegacias de polícia especializadas no enfrentamento do crime cibernético e os peritos em informática) recebam treinamento técnico constante para acompanhar a evolução tecnológica que ocorre quase que diariamente, e que tenham exato entendimento de como os criminosos atuam e quais os meios empregados por eles para a prática delituosa.

Esta circunstância desafia as concepções tradicionais sobre a natureza da prova, bem como sobre os mecanismos de identificação das evidências do crime e seu recolhimento para posterior valoração. Isto se dá, de acordo com o entendimento de Kist, pela razão de que a cibercriminalidade deixou para trás o ambiente físico e instalou-se em um ambiente digital e, por óbvio, é neste ambiente que também se encontram as provas dos crimes e é nele que deverão ser identificadas e dele recolhidas.<sup>89</sup>

---

<sup>88</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 117.

<sup>89</sup> *ibidem*, p. 106.

## 2.2.1 Meios de obtenção da prova no ambiente digital

Alguns dos principais meios de obtenção de prova no meio ambiente digital são: interceptação cibernética, infiltração no meio ambiente digital; busca e apreensão cibernética; as previsões trazidas pelo Marco Civil da *Internet*; e cooperação internacional.

A seguir serão estudados cada uma destas formas na tentativa de melhor entender como se dá a colheita de provas no enfrentamento à cibercriminalidade.

### 2.2.1.1 Interceptação cibernética

A Lei nº 9.296/96 traz em seu artigo 1º, parágrafo único, a previsão da interceptação do fluxo de comunicações em sistemas de informática e telemática, contemplando, portanto, esse meio de produção probatória. Trata-se aqui do acesso ao conteúdo da mensagem objeto de investigação durante sua transmissão, ou seja, em curso e em tempo real, pois caso o conteúdo que se almeja acessar já tiver sido transmitido ou ainda está em poder do emitente em momento anterior ao envio, outras medidas para a colheita da prova serão necessárias, e não mais a interceptação. Como bem nos ensina Kist:

(...) esta espécie de comunicação revela duas realidades que, embora interligadas e sequenciais, não se confundem: a primeira é a transmissão de mensagens que cria uma relação triangular a envolver o emitente e o destinatário da mensagem, ligados, entre si, pelo terceiro responsável pelo seu transporte (o prestador desse serviço); enquanto a mensagem estiver na posse desse terceiro ela pode ser acessada por alguém que não é o destinatário, e esse acesso configura a interceptação da comunicação telemática; a segunda realidade é aquela consistente em acessar o conteúdo transmitido por essa via depois de concluído o processo de comunicação; neste caso, já não há comunicação em curso e atual e, portanto, o conteúdo não é mais passível de interceptação; para conhecer esse conteúdo são necessárias outras medidas, que se concretizam pelo acesso à memória do dispositivo informático utilizado para a comunicação e na qual seu produto está armazenado, ou então na respectiva *cloud*, na qual os dados poderão estar em virtude de *backup* (cópia de segurança).<sup>90</sup>

A identificação do emitente/investigado se torna fundamental para que ocorra a interceptação de comunicação no ambiente digital, pois se realizada de forma indiscriminada, esta forma de obtenção de prova acarretará na violação do sigilo das comunicações privadas, assegurado no próprio artigo 5º, inciso XII da Constituição Federal que a Lei nº 9.296/96 regulamenta. A Lei determina, portanto, que a

---

<sup>90</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 251.



autorização para a interceptação será conferida com especificidade quanto àquele que está sendo investigado, a fim de evitar o acesso de conteúdo alheio e completamente dissociado do crime que está sendo apurado.

### 2.2.1.2 Infiltração no ambiente digital

Rafael Wolff ensina que agente infiltrado é aquele policial que, ocultando sua verdadeira identidade e função através do uso de identidade fictícia, aproxima-se de suspeitos da prática de determinados crimes para fazer prova de sua ocorrência.<sup>91</sup>

A legislação penal brasileira admite, em alguns casos, a infiltração policial em ambiente de crime, como a Lei nº 11.343/06<sup>92</sup> (lei de drogas) e a Lei nº 12.850/13<sup>93</sup> (crime organizado), podendo estes se darem da forma física ou digital. Já no tocante aos crimes cibernéticos, a Lei nº 13.441/17<sup>94</sup> prevê expressamente a infiltração por agentes de polícia no ambiente da *internet*. Referida lei estabelece este meio de obtenção de prova para os crimes alterados e acrescidos à Lei nº 8069/90 (Estatuto da Criança e do Adolescente) através da Lei nº 11.829/08<sup>95</sup>, que criminalizou condutas no enfrentamento à pornografia infantil e pedofilia.

Os crimes previstos nos artigos 240, 241, 241-A, 241-B, 241-C e 241-D<sup>96</sup> do ECA passaram então a prever como meio de obtenção de prova a infiltração na

---

<sup>91</sup> WOLFF, Rafael. Infiltração de agentes por meio virtual. In: SILVA, Ângelo Roberto Ilha da (org.). **Crimes cibernéticos**. 2. ed. Porto Alegre: Livraria do advogado, 2018, p. 218.

<sup>92</sup> BRASIL. **Lei nº 11.343, de 23 de agosto de 2006**. Artigo 53. Em qualquer fase da persecução criminal relativa aos crimes previstos nesta Lei, são permitidos, além dos previstos em lei, mediante autorização judicial e ouvido o Ministério Público, os seguintes procedimentos investigatórios: I – a infiltração por agentes de polícia, em tarefas de investigação, constituída pelos órgão especializados pertinentes; (...).

<sup>93</sup> BRASIL. **Lei nº 12.850, de 02 de agosto de 2013**. Artigo 3º. Em qualquer fase da persecução penal, serão admitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção de prova: (...) VII – infiltração por policiais, em atividade de investigação, na forma do art. 11; (...).

<sup>94</sup> BRASIL. **Lei nº 13.441, de 8 de maio de 2017**. Altera a Lei 8.609, de 13 de julho de 1990 (estatuto da criança e do adolescente), para prever a infiltração de agentes de polícia na *internet* com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

<sup>95</sup> BRASIL. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a lei nº 8.069, de 13 de julho de 1990 – Estatuto da criança e do adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na *internet*.

<sup>96</sup> BRASIL. **Lei nº 8.069, de 13 de julho de 1990**.

Artigo 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente;

Artigo 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente;

Artigo 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente;

*internet* realizada por agentes de polícia. Além dos crimes acima mencionados, o Código Penal também foi contemplado com a possibilidade de lançar mão do mesmo meio de prova em seus artigos 154-A, 217-A, 218, 218-A e 218-B.<sup>97</sup>

Diferentemente do ambiente físico, quando o agente infiltrado coloca sua integridade física em risco, no meio ambiente digital os desafios são outros, já que para ser aceito em ambiente de prática delituosa o agente deverá obter a confiança do grupo ao qual pretende se infiltrar, e caso não utilize os métodos e linguagens adequados àquela atividade, colocará em risco toda operação.

Neste caso, poderia o agente infiltrado ser responsabilizado por eventual conduta delituosa na tentativa de ingressar no ambiente de crime, não fosse a previsão do artigo 190-C<sup>98</sup> do ECA, que estabelece que o agente não cometerá crime quando oculta sua identidade para colher indícios e materialidade dos crimes previstos na lei, podendo, porém, ser responsabilizado pelos excessos praticados. Nos ensinamentos de Kist, quanto a participação de agente infiltrado em ambiente de crime:

Neste particular, e especificamente quanto às condutas que tipificam crimes de pedo-pornografia infantil, dado o caráter intrinsecamente ilícito desta atividade, é comum que ela seja desenvolvida em redes *peer-to-peer*, no interior de grandes grupos, cujos integrantes compartilham imagens e as consomem para a satisfação da lascívia; para que o policial consiga acesso

---

Artigo 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente; Artigo 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual;

Artigo 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso.

<sup>97</sup> BRASIL. **Código Penal Brasileiro. Decreto-Lei nº 2.848, de 7 de dezembro de 1940.**

Artigo 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;

Artigo 217-A. Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos ou com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência;

Artigo 218. Induzir alguém menor de 14 (catorze) anos a satisfazer a lascívia de outrem;

Artigo 218-A. Praticar, na presença de alguém menor de 14 (catorze) anos, ou induzi-lo a presenciar, conjunção carnal ou outro ato libidinoso, a fim de satisfazer lascívia própria ou de outrem;

Artigo 218-B. Submeter, induzir ou atrair à prostituição ou outra forma de exploração sexual alguém menor de 18 (dezoito) anos ou que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, facilitá-la, impedir ou dificultar que a abandone;

<sup>98</sup> BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Artigo 190-C. Não comete crime o policial que oculta sua identidade para, por meio da *internet*, colher indícios de autoria e materialidade nos crimes nos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do decreto-lei nº 2.848, de 7 de dezembro de 1940 (código penal). Parágrafo único. O agente policial infiltrado que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados.

a um grupo desses, como qualquer outro interessado, normalmente dele é demandada demonstração de que efetivamente é um pedófilo, exigindo-se que pratique atos que, ao menos formalmente, tipificam alguns dos crimes em questão, como disponibilizar ou transmitir fotografia que demonstre cena de sexo explícito envolvendo criança ou adolescente. Para além disso, e depois de admitido no grupo, é comum que seus integrantes promovam uma autovigilância para identificar eventuais intrusos, e o mecanismo é a observação daqueles que não transmitem fotografias/vídeos; disso decorre que o agente infiltrado num grupo desses é obrigado a participar das atividades nele desenvolvidas e para as quais ele existe, sob pena de ser excluído e, com isso, perder por completo a oportunidade de identificar os integrantes do grupo. Novamente, poderá ser demandado a praticar condutas que se amoldam a alguma figura típica.<sup>99</sup>

Há, portanto, o desafio do agente infiltrado em ser aceito numa rede de comunicação *peer-to-peer*<sup>100</sup>, adotando condutas que o faça exercer seu poder de convencimento para que não gere nenhum tipo de desconfiança dos demais integrantes do grupo, quando então ele terá a oportunidade de identificar os autores dos delitos.

Além disso, outro grande desafio na infiltração cibernética é o do agente que, ao compartilhar conteúdo ilícito com o objetivo de ser aceito no grupo criminoso, não venha a se tornar um agente provocador e iniciar um processo de instigação para que o crime se concretize. Neste caso estará o agente extrapolando seus limites como infiltrado e revestirá o procedimento investigatório de ilegalidade, gerando a não consumação do crime. Neste sentido a Súmula 145 do STF<sup>101</sup> é bastante clara quanto a este tipo de conduta por parte do policial: “Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação”.

No caso de o agente infiltrado provocar o surgimento do crime, o qual não seria praticado sem a sua intervenção, só restará à investigação a possibilidade do enquadramento de condutas anteriores à provocação. Como ensina Wolf:

Nada impede, por outro lado, que o flagrante seja aceito pela prática de crime em momento anterior à instigação. Logo, aquele que vende entorpecente a policial à paisana não pratica crime de tráfico de entorpecentes na modalidade vender, porque a troca da mercadoria por dinheiro jamais seria consumada. Ocorrerá, entretanto, o flagrante pelo fato de o investigado ter em depósito a substância, que já havia se consumado.

O mesmo raciocínio deve ser aplicado aos delitos virtuais. Utilize-se, como exemplo, o art. 241-A do Estatuto da Criança e do Adolescente (ECA), que pune oferecimento, troca, disponibilização, transmissão, distribuição,

---

<sup>99</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 271.

<sup>100</sup> Peer-to-peer (do inglês par a par ou simplesmente ponto a ponto, com sigla P2P): Trata-se de uma arquitetura de comunicação de computadores onde cada um dos pontos compartilha dados sem a necessidade de um servidor central.

<sup>101</sup> BRASIL. Superior Tribunal Federal. **Súmula 145**. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2119>. Acesso em: 05 out. 2020.

publicação ou divulgação “por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornografia envolvendo criança e adolescente”. Assim, se uma policial infiltrada, fingindo ser um senhor de meia idade, sugere troca de vídeo pornográfico infantil com investigado, este não poderá ser preso em flagrante pelo verbo nuclear trocar. Isto porque, por “ineficácia absoluta do meio”, o crime não irá se consumir (art. 17 do CP). O vídeo não entrará em circulação, nem correrá o risco de causar lesão ao bem jurídico tutelado, pois será apreendido pela polícia. Por outro lado, incidirá o agente no crime de armazenar ou possuir “fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornografia envolvendo criança ou adolescente” (art. 241-B do ECA). Afinal, no tocante a este, a atividade já havia se consumado, sem qualquer instigação do agente, diga-se de passagem.<sup>102</sup>

Como mencionado no início deste tópico, a legislação penal brasileira admite, em alguns casos, a infiltração policial em ambiente de crime, como prevê a Lei nº 11.343/06 (lei de drogas), a Lei nº 12.850/13 (crime organizado), e a Lei nº 13.441/17, que prevê expressamente a infiltração em investigações nos crimes alterados e acrescidos ao ECA no enfrentamento à pornografia infantil e pedofilia.

Ao analisar referidas hipóteses de infiltração em ambiente cibernético, nota-se que o prazo para este tipo de obtenção de prova estabelecido na Lei nº 13.441/17 não poderá exceder 90 dias, podendo ser prorrogado por até o limite de 720 dias. Na Lei nº 12.850/13 o prazo será de 6 meses, o qual poderá ser prorrogado por tempo indeterminado. Já a Lei nº 11.343/06 sequer estabelece um prazo limite para a infiltração.

O que se pretende demonstrar é o prejuízo que uma investigação de crimes contra a dignidade sexual da criança e do adolescente terá quando lançar mão da infiltração de agentes, comparada a uma investigação de tráfico de entorpecentes ou de organização criminosa. Qual teria sido a intenção do legislador quando estabeleceu prazo inferior de infiltração nos crimes previstos no ECA? Serão os bens jurídicos protegidos nesta Lei de menor relevância quando comparados àqueles cujos os prazos de infiltração são maiores?

A resposta parece clara, a infiltração cibernética nos crimes previstos no ECA certamente deveria dispor de um lapso temporal mais extenso para ser concluída. A investigação certamente seria mais eficiente, os agentes disporiam de prazos maiores para a identificação dos criminosos, e a consequência seria a melhora significativa dos índices de esclarecimentos destes tipos de delitos.

---

<sup>102</sup> WOLFF, Rafael. Infiltração de agentes por meio virtual. In: SILVA, Ângelo Roberto Ilha da (org.). **Crimes cibernéticos**. 2. ed. Porto Alegre: Livraria do advogado, 2018, p. 228.

### 2.2.1.3 Busca e apreensão cibernética

O meio de obtenção de prova consistente na busca e apreensão cibernética não encontra previsão legal em nosso ordenamento jurídico. Para lançar mão deste importante meio probatório, a investigação criminal deverá seguir o regramento previsto nos artigos 240 a 250 do Código de Processo Penal. Como ensina Kist, esta regulação, sabe-se, pressupõe que o objeto buscado e passível de apreensão se encontre no domicílio do investigado, dependendo a diligência de prévia autorização judicial, já que relativiza a inviolabilidade inerente a ele.<sup>103</sup>

Nada impede ainda que a busca e apreensão seja feita com base nos incisos II e III do artigo 6º<sup>104</sup> do mesmo Código, e portanto, tanto nas situações de prisões em flagrante, como nos casos da necessidade da realização de busca pessoal, se forem encontrados na posse dos suspeitos aparelhos informáticos que tenham alguma relação com o crime deverão ser apreendidos formalmente.

A busca, em ambos os casos descritos, é realizada com o intuito de apreender equipamentos e componentes de informática que possam conter dados relevantes à investigação, como computadores, *tablets*, *smartphones*, CDs, *pen drives*, HDs externos, etc., os quais serão encaminhados à perícia criminal informática para que então sejam identificadas e colhidas as informações de interesse e que servirão para compor o conjunto probatório. Diferentemente dos casos de interceptação cibernética, o conteúdo que comporá o conjunto probatório não estará em trânsito, sendo compartilhado entre os criminosos, e sim estará de posse destes, armazenados em dispositivos que serão objeto da busca e apreensão.

### 2.2.1.4 O Marco Civil da *Internet* e a obtenção da prova digital

O Marco Civil da *Internet*, introduzido pela Lei nº 12.965/14, estabeleceu os princípios, as garantias, os direitos e os deveres que envolvem os usuários, fornecedores de serviços e também o Estado, com o intuito de regulamentar o uso da *internet* no Brasil. Referida lei ainda dispõe sobre as formas que serão buscadas as provas digitais e também quais serão essas provas.

<sup>103</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 275.

<sup>104</sup> BRASIL. **Código de Processo Penal. Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Artigo 6º. Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: (...) II – apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; III – colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; (...).

Nos incisos II e III do artigo 7º<sup>105</sup> da Lei, que trata dos direitos e garantias dos usuários, verifica-se a possibilidade de requisitar tanto os dados em fluxo quanto os armazenados, e sempre mediante ordem judicial, devendo sua aplicação se dar conforme as disposições da Lei nº 9.296/96, já estudada anteriormente no tópico sobre interceptação cibernética.

Augusto Tavares Rosa Marcacini, ensina que a lei fez a correta distinção entre dados digitais estáticos, que se encontram armazenados em algum banco de dados ou dispositivo de armazenamento, dos dados que se encontram em trânsito, e possam ser captados durante o estabelecimento da comunicação.<sup>106</sup>

Além dos dois princípios gerais previstos no artigo 7º, o Marco Civil da *Internet* estabelece ainda outras disposições, que estão previstas no artigo 10, parágrafos 1º e 2º<sup>107</sup>, tratando de que a disponibilização dos registros de conexão<sup>108</sup> e registros de acesso a aplicações de *internet*<sup>109</sup> (*logs*<sup>110</sup>), e do conteúdo de comunicações privadas serão disponibilizados pelo provedor responsável pela guarda e registro mediante ordem judicial.

Jesus e Milagre acrescentam que do mesmo modo, a remoção de conteúdos só será possível também mediante uma ordem judicial, com exceção dos casos envolvendo fotos de nudez, quando a mera notificação extrajudicial deverá ser

---

<sup>105</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Artigo 7º. O acesso à *internet* é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) II – inviolabilidade e sigilo do fluxo de suas comunicações pela *internet*, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (...).

<sup>106</sup> MARCACINI, Augusto Tavares Rosa. Provas digitais: limites constitucionais e o marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei nº 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 468.

<sup>107</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Artigo 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

Parágrafo 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitando o disposto no art. 7º.

Parágrafo 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitando o disposto nos incisos II e III do art. 7º. (...).

<sup>108</sup> Registro de conexão é o conjunto de informações referentes à data e hora de início e término de uma conexão à *internet*, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.

<sup>109</sup> Registros de acesso a aplicações de *internet* são o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de *internet* a partir de um determinado endereço IP.

<sup>110</sup> No meio informático, *log* é a expressão usada para descrever o processo de registro num sistema de computadores.

atendida pelos provedores de conteúdo,<sup>111</sup> isto conforme prevê o artigo 21 da Lei<sup>112</sup>, sob pena de responsabilização subsidiária.

Quanto aos dados de conteúdo mencionados no parágrafo 2º do artigo 10, importante salientar que tratam-se aqui dos dados que já foram enviados e chegaram ao seu destinatário, encontrando-se armazenados em algum dispositivo informático, seja o do emitente, o do próprio destinatário ou ainda o do provedor responsável pela guarda, que provavelmente ainda as mantém registradas ou armazenadas, dependendo da possibilidade técnica que pode variar de empresa para empresa, o que poderá inviabilizar o fornecimento das comunicações realizadas. A ausência de registro dos conteúdos que passam pelo banco de dados dos provedores por certo acarreta prejuízo a futuras investigações criminais, que não poderão contar com essas informações para compor o conjunto probatório ideal. Neste sentido, nos ensinamentos de Kist:

Quando e desde que haja comprovação técnica nesse sentido, ou seja, de que a comunicação mantida por particulares, ao passar pelos servidores da dita empresa, ali não fica registrada ou armazenada, efetivamente não há como exigir dela que exiba os referidos registros, pois não os têm. Poder-se-ia cogitar, por exemplo, de uma obrigação das empresas no sentido de registrar e armazenar o conteúdo que passa por seus servidores, com a finalidade de obtê-lo posteriormente, quando necessário para a investigação criminal; contudo, uma tal exigência deveria ser vertida em lei; inexistente esta, não há como opor-se à opção da empresa em não fazer o registro, decisão que por certo integra seu plano de negócios e seu modo de atuar no mercado.<sup>113</sup>

Há portanto a problemática de que ordens judiciais que determinem o fornecimento do conteúdo de comunicações privadas se tornem inócuas, uma vez que a alegação das empresas em não possuírem capacidade técnica para o armazenamento de todo o conteúdo que passa por seus servidores inviabilize o cumprimento da referida ordem.

---

<sup>111</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 171.

<sup>112</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Artigo 21. O provedor de aplicações de *internet* que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

<sup>113</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 261.

No mesmo artigo, o parágrafo 3º<sup>114</sup> ainda estabelece que o acesso aos dados cadastrais, como nome, filiação e endereço poderão ser obtidos por autoridades administrativas, como os Delegados de Polícia e membros do Ministério Público, mediante a simples requisição encaminhada diretamente aos provedores de acesso.

Bastante pertinente os ensinamentos de Marcacini quanto a fragilidade dos registros de conexão como provas digitais de forma isolada, necessitando a complementação com outros tipos de provas para atender as necessidades da persecução processual:

É evidente que tais *logs* representam nada mais do que meros indícios para se iniciar uma investigação mais profunda, ou para se requisitar judicialmente outras provas do ilícito civil ou penal. A fragilidade desses *logs* como prova, isoladamente considerada, decorre do fato de que são registros digitais potencialmente adulteráveis, passíveis de erros gerados pelo sistema que os produz, como ocorre com qualquer sistema informático, não sendo de se desconsiderar a hipótese, bastante palpável, de que um criminoso digital logre ele próprio adulterar tais registros, em caso de invasão de sistemas, ou mesmo que agentes do ambiente interno desses provedores cometam os ilícitos e tenham o poder fático de refazer os ditos *logs*, apontando-os para outros usuários da rede. A comparação prática possível, que costumamos fazer acerca desses *logs*, é que não são mais palpáveis do que uma pegada deixada no jardim do local do crime. São, sem dúvida alguma, importantes para o início de uma investigação e para fundamentar novas medidas judiciais tendentes a obtenção de outras provas. Isoladamente, porém, é uma prova demasiadamente frágil para sustentar uma decisão judicial, tanto penal como civil.<sup>115</sup>

Quanto aos prazos para que os provedores mantenham guardados os registros de conexão e os registros de acesso a aplicações de *internet*, o Marco Civil da *Internet* estabelece que serão, respectivamente, de um ano, previsto no artigo 13<sup>116</sup>, e de seis meses, previsto no artigo 15<sup>117</sup>, podendo ambos serem guardados por

<sup>114</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Artigo 10. (...). Parágrafo 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. (...).

<sup>115</sup> MARCACINI, Augusto Tavares Rosa. Provas digitais: limites constitucionais e o marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei nº 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 471.

<sup>116</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Artigo 13. Na provisão de conexão à *internet*, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (...).

Parágrafo 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

<sup>117</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Artigo 15. O provedor de aplicações de *internet* constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a



prazo superior, desde que por ordem judicial, requerida pela autoridade policial ou membro do MP. Consta ainda no caput do artigo 22<sup>118</sup> da Lei nº 12.965/14 que, em caso de necessidade para que se forme o conjunto probatório em processos judiciais, tanto na esfera cível quanto penal, a parte interessada poderá requisitar ao juiz que ordene ao responsável pela guarda o fornecimento dos registros de conexão ou dos registros de acesso a aplicações de *internet*.

Referido artigo não menciona os registros que compõem os dados cadastrais, porém, como já estudado anteriormente no parágrafo 3º do artigo 10, as autoridades administrativas poderão requisitar o fornecimento desses dados diretamente aos provedores de acesso. Caso o interessado seja um particular, nada impede que ele requeira ao juiz para que especifique a ordem de fornecimento. No mesmo sentido, nos ensinamentos de Kist:

Quanto aos dados cadastrais, ainda que não mencionado no artigo 22, nada impede sua requisição judicial; é claro que se a “*parte interessada*” no conhecimento desses dados seja uma das autoridades antes referidas, elas podem requisitar de forma direta o seu fornecimento ao responsável pela guarda. Mas, caso se trate de particular, o fornecimento deve ser requerido ao juiz que por sua vez, o requisitará.<sup>119</sup>

Concluindo ainda os estudos sobre o Marco Civil da *Internet*, para que a ordem judicial seja expedida, deve-se comprovar os indícios da ocorrência do ilícito, a importância que os registros solicitados têm para comporem o conjunto probatório, além da especificação exata do período ao qual se referem os registros.

### 2.2.1.5 Aplicações de comunicação instantânea

A maneira como as pessoas se comunicam tem sofrido grande mudança ao longo dos tempos. Já vivenciamos diversos meios pelos quais as mensagens eram enviadas, dentre as quais pode-se destacar o uso de pessoas como seus portadores, as cartas escritas e os telegramas, enviados através do serviço de correios, além do telefone fixo e do telégrafo, dentre outros. Na atualidade, diante do surgimento da

---

aplicações de *internet*, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (...).

Parágrafo 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de *internet* que os registros de acesso a aplicações de *internet* sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.

<sup>118</sup> BRASIL. Lei nº 12.965, de 23 de abril de 2014. Artigo 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de *internet*.

<sup>119</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 258.

sociedade da informação e o acesso aos meios de comunicação ligados à *internet*, as aplicações de comunicação instantânea se tornaram uma das principais alternativas para a troca de informações entre as pessoas, como por exemplo, o *Signal*, o *Telegram*, e o *WhatsApp*, este último certamente o mais popular de todos.

Referidos sistemas de comunicação se tornaram muito atraentes pelo fato de serem gratuitos, de linguagem simples, e o mais importante, permitem a troca instantânea de mensagens, colocando duas pessoas ou um grupo de pessoas numa mesma conversa e em contato ininterrupto em frações de segundos. Quanto as aplicações de comunicação instantânea, nos ensinamentos de Kist:

É notório que essas ferramentas incrementaram os atos comunicacionais em termos quantitativos – em número (com mais pessoas) e em frequência (mais vezes com a mesma pessoa), o que, por si, é um fator indutor da criação de laços mais próximos entre as pessoas, que poderão inclusive conduzir à própria intimidade. A isso é de acrescentar a simplificação dos processos de comunicação, o que foi uma das principais causas da sua disseminação, não havendo barreiras de matriz intelectual para o manejo dos dispositivos e aplicativos. Ainda, há nesses mecanismos uma multiplicidade de funções, que os tornam atrativos; permitem que as pessoas, ao mesmo tempo, troquem, entre si, mensagens escritas e áudios, mandem arquivos e fotografias, tudo numa velocidade incrível e que despreza totalmente a distância física eventualmente existente entre elas.<sup>120</sup>

A grande problemática é que, da mesma maneira que essas aplicações auxiliam a todos em suas tarefas diárias, abre-se também um precedente para a prática delituosa, onde os criminosos, aproveitando-se da popularidade e disseminação deste tipo de aplicação, passaram também a atuar fazendo uso dos mesmos. Kist complementa ensinando que:

Pode-se mesmo falar, em contexto mais amplo, em uma criminalidade informático-digital ou cibercriminalidade, pois os criminosos não ficaram inertes diante das novas tecnologias de comunicação impulsionadas pela Internet e ao ciberespaço; pelo contrário, passaram a utilizar-se desses recursos para organizarem-se e aprimorarem a atividade criminosa; e esses mesmos meios foram e vêm sendo utilizados pelos criminosos para anonimizarem-se, esconderem-se e esquivarem-se da atuação estatal preventiva e repressiva do crime. É natural que, num contexto destes, manifesta-se a necessidade de novas medidas investigatórias e adaptação do Direito Processual Penal, notadamente porque a tradicional prova material ou física cede lugar à prova digital; conseqüentemente, os meios clássicos de obtenção de prova, talhados para atuar no mundo físico, apresentam-se como insuficientes para a investigação destes crimes, cuja evidência situa-se no mundo digital.<sup>121</sup>

É neste contexto que entra aqui a análise de como esses tipos de aplicações podem contribuir para a formação de um conjunto probatório relevante para a

<sup>120</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 353.

<sup>121</sup> *ibidem*, p. 329.

persecução penal. Quando uma aplicação de comunicação instantânea é utilizada, três são as opções pelas quais um conteúdo poderá ser enviado através da *internet*.

A primeira delas é a possibilidade de a comunicação ser estabelecida através do sistema VoIP<sup>122</sup>, que se dará como uma ligação através de um aparelho de telefone convencional. Como Kist descreve, essa forma de comunicação, ao menos no aspecto externo, em tudo se assemelha à tradicional conversa telefônica, em que dois interlocutores mantêm conversação atual, usando-se dos serviços de um terceiro, que viabiliza, tecnicamente, esta comunicação.<sup>123</sup> Estaremos diante, portanto, dos casos da interceptação cibernética, prevista na Lei nº 9.296/96.

A segunda diz respeito ao conteúdo escrito, que consiste na troca de mensagens de textos, fotos, vídeos e até mesmo gravações de áudio. Nos ensinamentos de Kist, questão que pode ofertar alguma dificuldade é saber se o regime da interceptação telefônica tem capacidade para regular a interferência na transmissão, pelo aplicativo em questão, de mensagens escritas, vídeos, imagens e arquivos diversos, incluindo áudios.<sup>124</sup> Trata-se aqui de uma comunicação em curso, onde há a figura de um emissor da mensagem, de um receptor, e também de um terceiro que viabiliza o envio da comunicação entre os dois primeiros.

As mensagens, ao serem emitidas e antes de chegarem ao seu destino, estarão na posse do aplicativo, e poderão ser objeto de uma intervenção externa, podendo ser interceptadas, nos mesmos moldes de uma ligação telefônica tradicional ou por VoiP, aplicando-se, portanto, o regime previsto pela Lei nº 9.296/96. Há a evidente semelhança deste tipo de comunicação com a tradicional ligação telefônica, e a interceptação passa a ser a alternativa viável para a colheita da prova, conforme ensina Kist:

A semelhança com a interceptação da comunicação telefônica reside exatamente nisso: a intromissão ocorre durante o período em que a mensagem transita pelos sistemas utilizados para o transporte e entrega, ou seja, enquanto ela está sob o domínio do terceiro/empresa para a transmissão. A dessemelhança situa-se no fato de não se tratar da interceptação de “palavra falada”, e, sim, de palavra escrita.<sup>125</sup>

---

<sup>122</sup> VoIP ou voz sobre protocolo de *internet* é a tecnologia que permite a conversação humana usando a *internet* ou uma rede de computadores baseada no Protocolo de *Internet*, o que torna a transmissão de voz mais um dos múltiplos serviços suportados pela rede de dados.

<sup>123</sup> KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019, p. 339.

<sup>124</sup> *ibidem*, p. 340.

<sup>125</sup> *ibidem*

Em resumo, tanto a interceptação da comunicação da palavra falada, realizada pelo sistema VoIP, como a interceptação da comunicação escrita, através do envio de textos, fotos, vídeos, etc., estarão sujeitas à aplicação da Lei nº 9.296/96.

Enfim, a terceira e última se relaciona com os conteúdos que já foram transmitidos e encontram-se armazenados nos respectivos dispositivos utilizados para a comunicação. Portanto, o objeto agora não é mais a mensagem que está em fluxo, a caminho de seu destinatário e sob o domínio das empresas terceiras responsáveis por viabilizar a transmissão, e sim a mensagem que já está na posse de quem a recebeu, que depois de acessada e visualizada, estará armazenada na memória do dispositivo informático utilizado.

Em síntese, já não se trata de captar o teor de uma comunicação em processamento, e sim, de acessar dados que se encontram guardados em suporte digital; já não é o caso de escutar palavras faladas por meio de telefone, de interceptar um *e-mail* que esteja a caminho da caixa de mensagens do correio eletrônico de alguém ou das mensagens escritas que dois interlocutores estejam trocando por meio do *WhatsApp*; a hipótese agora é a de acessar tais comunicações depois que elas ocorreram, acessando a memória dos dispositivos eletrônicos (computador, *tablet* ou *smartphone*) utilizados para a transmissão.

Estaremos, portanto, diante dos casos de busca e apreensão, conforme o regramento previsto nos artigos 240 a 250 do Código de Processo Penal. Como já estudado anteriormente, os requisitos para viabilizar a busca e apreensão serão de que o objeto buscado e passível de apreensão se encontre no domicílio do investigado, além da necessidade de prévia autorização judicial.

A busca e apreensão poderá ser realizada com base nos incisos II e III do artigo 6º do mesmo Código, e portanto, tanto nas situações de prisões em flagrante, quanto nos casos da necessidade da realização de busca pessoal, os equipamentos informáticos que tenham alguma relação ou suspeita de relação com o crime objeto da investigação deverão ser apreendidos.

A grande dificuldade que os agentes públicos encontram quando realizam uma investigação cibernética cujo conjunto probatório provavelmente será encontrado em aplicações de comunicação instantânea é o fato desses aplicativos disporem de

tecnologia de criptografia<sup>126</sup>, impondo grande dificuldade técnica para que sejam obtidos resultados favoráveis à investigação. Neste caso, a tentativa será a de interceptar o conteúdo das mensagens do emitente antes da codificação ou do destinatário depois da descodificação, o que dificulta demasiadamente o trabalho da interceptação.

### 2.2.1.6 Cooperação internacional

Com o objetivo de estabelecer uma regulamentação comum e ações conjuntas entre países no tocante ao enfrentamento dos crimes cibernéticos, no ano de 2001 foi firmado pelo Conselho da Europa a Convenção do Cibercrime,<sup>127</sup> que criminaliza diversas condutas ilícitas praticadas na *internet*, além de possibilitar a cooperação internacional na identificação e colheita de provas nos crimes que tenha como uma de suas características a transnacionalidade. Como mencionado anteriormente, a Convenção de Budapeste será mais bem estudada no Capítulo 3 deste trabalho, mais especificamente no tópico 3.3.

Todos que atuam diretamente no enfrentamento ou de alguma forma colaboram para minimizar a incidência dos crimes cibernéticos entendem que este é um importante instrumento para auxiliar a persecução penal, e em se tratando de colheita de prova, seria um grande avanço para o Brasil poder contar com a colaboração de outros países signatários nos casos em que os crimes extrapolem os limites territoriais brasileiros. Neste sentido, Francisco Rezek e Guilherme Berti de Campos Guidi assim ensinam sobre os desafios da colheita de provas:

Em termos objetivos, as características da Internet – sobretudo sua descentralização e sua distribuição indistinta por diversos territórios – nos impõem sérios desafios quando se trata de investigar, julgar e unir uma conduta criminosa. As provas de tais condutas, da materialidade e da autoria do crime, podem encontrar-se em máquinas a milhares de quilômetros de onde os efeitos do crime foram sentidos, ou de onde a conduta deve ser julgada.<sup>128</sup>

---

<sup>126</sup> Criptografia é a técnica utilizada para proteger informações e comunicações através do uso de códigos e cálculos baseados em algoritmos, que transformam mensagens enviadas, de modo que apenas seu destinatários possam acessá-las, impedindo assim a interferência de terceiros

<sup>127</sup> CONVENÇÃO SOBRE O CIBERCRIME. **Convenção de Budapeste. 2001.** Disponível em [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf). Acesso em: 17 jul. 2019.

<sup>128</sup> GUIDI, Guilherme Berti de Campos; REZEK Francisco. Crimes na *internet* e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 278.

Atualmente, para contar com a cooperação internacional em casos de crimes cibernéticos, por ser signatário do MLAT<sup>129</sup>, o Brasil poderá valer-se de carta rogatória para obter a colheita de provas. Guidi e Rezek assim ensinam:

A carta rogatória consiste no mais básico instrumento de cooperação internacional. Trata-se de pedido feito pelo Judiciário de um país ao de outro Estado, rogando-lhe que dê execução aos atos ordenados na decisão original, sejam eles de comunicação ou instrução processual. Entre aqueles, podemos incluir as citações e as intimações de atos judiciais, entre estes a colheita de provas em geral, como a oitiva de testemunhas, a apreensão de documentos, o interrogatório do réu, etc.<sup>130</sup>

Este procedimento é realizado através do Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI) do Ministério da Justiça e Segurança Pública, que faz a intermediação entre os países signatários e que foram envolvidos num crime cibernético. Nos ensinamentos de Jesus e Milagre:

Neste caso, o delegado que está conduzindo a investigação representa ao juiz, e de posse da resposta do juiz autorizando a quebra, ele entra em contato com o DRCI. Este, por sua vez, pode devolver a solicitação ao delegado, para que ela seja adaptada às necessidades do país que receberá a solicitação ou, caso esteja tudo em ordem e na língua do Estado de destino, encaminha ao país onde se buscam os dados de um criminoso digital ou a remoção de um conteúdo ilícito.<sup>131</sup>

Há casos em que a cooperação não se concretiza, isto decorrente da possibilidade de que o pedido brasileiro seja negado pelo país estrangeiro, sob a alegação de interferência na sua soberania. Guidi e Rezek complementam que por regra, não admite o soberano que outros pretendam dizer ou mandar no território onde exerce seu poder, mas pode o Estado, mediante comprometimento igualitário, escolher suportar algum grau de ingerência equivalente a fim de ter suas prerrogativas expandidas em relação à outra parte.<sup>132</sup>

Superado algum óbice relacionado à soberania, e atendida a carta rogatória, as informações solicitadas retornam ao DRCI para encaminhamento posterior ao órgão solicitante. Nos ensinamentos de Fernanda Teixeira Souza Domingos:

Ainda há a resistência por parte dos provedores estrangeiros de aplicações de Internet em atender à legislação brasileira em muitos aspectos sob a alegação de que determinadas informações e procedimentos se regem por

---

<sup>129</sup> MLAT (*Mutual Legal Assistance Treaty*) é um tratado internacional de assistência mútua em matéria penal, e que é estabelecido entre dois ou mais países, e que cria um procedimento de cooperação.

<sup>130</sup> GUIDI, Guilherme Berti de Campos; REZEK Francisco. Crimes na *internet* e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 282.

<sup>131</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 179.

<sup>132</sup> GUIDI, Guilherme Berti de Campos; REZEK Francisco. Crimes na *internet* e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 280.

outras jurisdições que não a brasileira, alegando ainda ser necessário um procedimento formal de cooperação internacional para que as provas possam ser validamente transferidas às autoridades brasileiras de investigação.<sup>133</sup>

Percebe-se, portanto, o quão burocrático e moroso é o procedimento da carta rogatória através do MLAT, o que certamente compromete a investigação, podendo as provas que servirão para uma persecução penal mais efetiva serem perdidas ou excluídas pelos provedores, resultando na impunidade dos criminosos. Domingos ressalta que, quando os órgãos de investigação e processamento optarem por se utilizar dos procedimentos de cooperação internacional para obter provas digitais esse trâmite precisa ser célere, sob pena de as provas se perderem ou de não servirem mais ao seu propósito.<sup>134</sup>

Fiorillo e Conte ainda descrevem que a cooperação internacional e a harmonização das legislações penais dos países despontam como saídas eficazes no combate à criminalidade informática, na medida em que permitem maior agilidade e eficácia nas investigações e punições.<sup>135</sup>

O Ministério Público Federal, através do Grupo de Apoio sobre Criminalidade Cibernética, em agosto de 2018 emitiu nota técnica endereçada à Secretaria de Cooperação Internacional do Ministério das Relações Exteriores<sup>136</sup>, enumerando diversos pontos que beneficiariam a justiça brasileira com o ingresso do país na Convenção, porém o referido documento ainda não surtiu efeito, e teremos que aguardar até que a adesão seja efetivada e que produza os resultados esperados.

Constata-se, portanto, que a adesão do Brasil à Convenção de Budapeste trará vários benefícios para o enfrentamento à criminalidade cibernética em nosso país, e em virtude das características de plurilocalidade e transnacionalidade dos crimes cibernéticos, a cooperação dos países aderentes se mostra essencial para o melhor desempenho da aplicação da legislação penal brasileira.

---

<sup>133</sup> DOMINGOS, Fernanda Teixeira Souza. A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual infantil *online*. In: SILVA, Ângelo Roberto Ilha da (org.). **Crimes cibernéticos**. 2. ed. Porto Alegre: Livraria do advogado, 2018, p. 252.

<sup>134</sup> *ibidem*

<sup>135</sup> FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2. ed., São Paulo: Saraiva, 2016, p. 310.

<sup>136</sup> BRASIL. Ministério Público Federal. **Nota técnica do grupo de apoio sobre criminalidade cibernética sobre a convenção de cibercrimes. (Convenção de Budapeste)**. 2018. Disponível em: [http://www.mpf.mp.br/pgr/documentos/2CCR\\_NotaTecnica\\_ConvencaoBudapeste.pdf](http://www.mpf.mp.br/pgr/documentos/2CCR_NotaTecnica_ConvencaoBudapeste.pdf). Acesso em: 07 out. 2019.

### 2.2.2 Deep Web e Dark Web

As atividades de investigação policial que envolvem os crimes cibernéticos, como se constata até o momento, deparam-se com inúmeros desafios diante do aperfeiçoamento da tecnologia e o surgimento de novos meios de execução das condutas ilícitas que são adotados pelos criminosos. Na tentativa constante de se esquivar da persecução penal, o cibercriminoso busca alternativas que impedem sua identificação e, por consequência, sua responsabilização pelos crimes que pratica.

Como ensinam Alesandro Gonçalves Barreto, Emerson Wendt e Guilherme Caseli:

No dia a dia da atividade de persecução penal exercida pelas polícias judiciárias, é comum verificar o aperfeiçoamento de técnicas e meios de execução das atividades ilícitas por parte dos criminosos que a todo momento procuram meios para se esquivar da atuação policial. Assim, em um primeiro momento, criminosos que atuavam em campo de realidade começaram a migrar suas formas de execução para o universo da Internet, visando ampliar seu mercado de atuação e, ainda, driblar a atuação das forças policiais. Hoje, esses mesmos criminosos estão mudando seu cenário de atuação para o conteúdo da deep web, por acreditarem no absoluto anonimato, bem como na falta de capacitação dos agentes de investigação.<sup>137</sup>

Dentre os meios utilizados para esta finalidade, a navegação em áreas da *internet* onde se torna quase impossível a identificação do usuário tem sido um dos métodos preferidos dos criminosos, onde o que se busca é a tentativa do absoluto anonimato. A área da *internet* mencionada refere-se à *Deep Web* ou *internet* profunda, que é a parte da rede cujo conteúdo não está disponível ou indexado em ferramentas de pesquisa como, por exemplo, Google, Yahoo, Bing, etc.

Estudo realizado pelos pesquisadores e especialistas em segurança da informação Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle e Martin Rosler, para a Trend Micro Incorporated, empresa global que atua exclusivamente neste segmento, ensinam assim sobre a *Deep Web*:

A Deep Web se refere a qualquer conteúdo da Internet que, por vários motivos, não pode ser ou não é indexado por mecanismos de pesquisa como o Google. Esta definição inclui páginas da web dinâmicas, sites bloqueados (como aqueles que pedem que você responda a um CAPTCHA para acessar), sites desvinculados, sites privados (como aqueles que exigem credenciais de login), conteúdo não HTML / contextual / com script e limitado - redes de acesso.<sup>138</sup>

<sup>137</sup> BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELI, Guilherme. **Investigação digital em fontes abertas**. 2. ed. Rio de Janeiro: Brasport, 2017, p. 208.

<sup>138</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web**. Trend Micro Incorporated. Disponível em:



Diferentemente da *Surface Web*, ou *internet* de superfície, onde os endereços eletrônicos são indexados aos sites de busca (a *Surface Web* representa uma fração muito pequena dos acessos à *internet* quando comparada aos acessos na *Deep Web* e *Dark Web*), na *Deep Web*, por diversas razões, o usuário não terá o livre acesso ao seu conteúdo. Dentre as razões pelas quais um conteúdo não é indexado ou localizado por ferramentas tradicionais de busca estão os casos de necessidade de acesso através de *login* e senha, algum tipo de bloqueio pelo próprio criador da página, ou ainda a necessidade de programas específicos de computador para se ter o acesso.

Na *Deep Web*, portanto, as páginas apenas não são indexadas, e são tranquilamente acessadas, o que gera equívocos na forma de interpretação por parte dos usuários, fazendo com haja a percepção de que está sendo empregada uma conduta ilícita ao acessar esta área da *internet*. Além das páginas não indexadas, mas acessíveis, a *Deep Web* ainda abrange uma área da *internet* mais privativa e com a característica da navegação em total anonimato, a chamada *Dark Web*.<sup>139</sup>

Na *Dark Web* as páginas não são acessadas pelas formas convencionais de uso, e há a necessidade de *softwares* específicos para acesso, transformando uma navegação convencional em uma navegação totalmente criptografada e anônima. E é justamente nesta área de acesso da *internet* que se encontram os maiores problemas, pois boa parte do conteúdo lá disponível tem alguma relação com atividades ilícitas. Ciancaglioni, Balduzzi, McArdle e Rosler complementam ensinando que:

Uma pessoa inteligente que compra drogas recreativas online não gostaria de digitar palavras-chave relacionadas em um navegador normal. Ele / ela precisará ficar online anonimamente usando uma infraestrutura que nunca levará as partes interessadas a seu endereço IP ou localização física. Os vendedores de drogas não gostariam de abrir uma loja em um local online cujo responsável pelo registro possa facilmente ser determinado ou onde o endereço IP do site está no mundo real.<sup>140</sup>

---

[https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 5. *The Deep Web refers to any Internet content that, for various reasons, can't be or isn't indexed by search engines like Google. This definition thus includes dynamic web pages, blocked sites (like those that ask you to answer a CAPTCHA to access), unlinked sites, private sites (like those that require login credentials), non – HTML/ - contextual/ - scripted content, and limited – access networks.*

<sup>139</sup> Imagem 01 do Anexo A, p. 123.

<sup>140</sup> CIANCAGLIONI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 6. Texto original: *A smart person buying recreational drugs online wouldn't want to type relate keywords*

Na *Dark Web* é comum ocorrer a comercialização de entorpecentes, a prática de pedofilia, a realização de fraudes bancárias e de operadoras de crédito, o comércio de documentos falsos, inclusive passaportes, a prática de atos terroristas, e até a contratação de assassinos de aluguel.

A forma de navegação neste ambiente se dá através de ferramentas específicas, e que normalmente não deixam rastros, tornando a navegação anônima, como é o caso do TOR (estudado no tópico seguinte), e a forma de pagamento utilizada para as transações comerciais será sempre a moeda digital, o *Bitcoin*<sup>141</sup>, (também estudada em tópico adiante).

### 2.2.2.1 Navegação anônima – TOR

O projeto TOR é uma ferramenta gratuita de navegação anônima, e que está disponível para *download* a todos aqueles que desejam navegar na *internet* com privacidade e sem ser identificado.

Nos anos 1990, a falta de segurança na internet e a possibilidade de usá-la para rastreamento e vigilância estavam se tornando claras. Em 1995, David Goldschlag, Mike Reed e Paul Syverson, no Laboratório de Pesquisa Naval dos EU (U.S. Naval Research Lab – NRL) perguntaram-se se havia uma maneira de criar conexões com a Internet que não revelassem quem estava falando com quem, nem mesmo a alguém que monitorasse a rede. A resposta deles foi criar e implantar os primeiros projetos de pesquisa e protótipos do roteamento onion.

O objetivo do roteamento onion era ter uma forma de usar a Internet com o máximo de privacidade possível, e a ideia era rotar o tráfego por múltiplos servidores e criptografá-lo a cada passo do caminho.<sup>142</sup>

O anonimato oferecido pela ferramenta TOR é obtido através da criptografia do conteúdo, que é percorrido por um caminho totalmente desconhecido da rede, utilizando para isso diversos servidores diferentes.

Sua criação e manutenção se deu e ainda se mantém de forma lícita, cujo objetivo principal era o de usuários não serem submetidos a qualquer tipo de censura, navegando de forma livre e com total privacidade. Originalmente quem mais se

---

*into a regular browser. He / She will need to anonymously go online using an infrastructure that will never lead interested parties to his / her IP address or physical location. Drug sellers wouldn't want to set up shop in an online location whose registrant law enforcement can easily determine or where the site's IP address exist in the real world, too.*

<sup>141</sup> Bitcoin, de uma forma bem sucinta, é uma criptomoeda descentralizada, que é utilizada como uma espécie de dinheiro eletrônico, sem que haja a interferência de instituições financeiras ou governamentais.

<sup>142</sup> Projeto TOR. **História**. Disponível em: <https://www.torproject.org/pt-BR/about/history/>. Acesso em: 19 jul. 2019.

beneficiou com o TOR foram os ativistas de países que vivem em regimes ditatoriais, cujo propósito era poder se comunicar, expressar suas opiniões e não serem identificados, o que os livraria de sofrer diversas sanções impostas pelo regime. Ciancaglili, Balduzzi, McArdle e Rosler ensinam as razões pelas quais pessoas comuns recorrem a ferramenta TOR em busca de anonimato e privacidade:

Existem muitas razões, além da compra de drogas, pelas quais as pessoas desejam permanecer anônimas ou criar sites que não podem ser rastreados até um local físico ou entidade. Pessoas que desejam proteger suas comunicações da vigilância do governo podem exigir a cobertura de darknets. Os denunciantes podem querer compartilhar uma grande quantidade de informações privilegiadas com jornalistas sem deixar rastros de papel. Dissidentes em regimes restritivos podem precisar do anonimato para permitir que o mundo saiba com segurança o que está acontecendo em seu país.<sup>143</sup>

Ocorre que a facilidade de uso e a vantagem de navegação anônima gerou o interesse por parte dos criminosos para a prática de atividades ilícitas na *Dark Web*, gerando dificuldades à investigação ainda maiores do que aquelas já conhecidas no ambiente virtual. Nos ensinamentos de Barreto, Wendt e Caseli:

Tendo em vista a complexidade do funcionamento de sua conexão, serviço e sistemática peculiar, é comum encontrar a difusão na mídia de que os nós de conexão realizados pela rede Tor torna a identificação do usuário completamente anônima. Mediante tal pseudoconstatação, a *deep web* se torna um ambiente propício para a proliferação de criminosos virtuais e *hacktivistas*.<sup>144</sup>

A identificação de criminosos nesta área da *internet* se mostra extremamente complexa e desafiadora, pois além do conteúdo ilícito ser criptografado, há ainda a problemática da utilização de diversos servidores diferentes para a comunicação, podendo estes, quando e se identificados, estarem localizados em diversos países, gerando então os conflitos de jurisdição anteriormente já estudados no tópico da cooperação internacional. Quanto aos desafios gerados pela navegação na *Deep Web*, Ciancaglili, Balduzzi, McArdle e Rosler acrescentam ensinando que:

As agências de aplicação da lei já enfrentam vários desafios existentes no que diz respeito ao crime internacional na Surface Web. Com relação à Deep

<sup>143</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web**. Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 6. Texto original: *There are many reasons, apart from buying drugs, why people would want to remain anonymous or set up sites that can't be traced back to a physical location or entity. People who want to shield their communications from government surveillance may require the cover of darknets. Whistleblowers may want to share vast amounts of insider information to journalists without leaving a paper trail. Dissidents in restrictive regimes may need anonymity in order to safely let the world know what's happening in their country.*

<sup>144</sup> BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELI, Guilherme. **Investigação digital em fontes abertas**. 2. ed. Rio de Janeiro: Brasport, 2017, p. 211.

Web, três aspectos adicionais podem tornar a aplicação da lei ainda mais problemática.

- Criptografia: Tudo na Deep ou Dark Web é criptografado. Isso significa que os criminosos estão muito mais conscientes sobre serem presos ou monitorados. A criptografia é a primeira contramedida para evitar a detecção.

- Atribuição: é extremamente difícil determinar a atribuição. Tudo acontece em domínios .onion. O roteamento para esses domínios também não está claro.

- Flutuação: A Deep Web é um lugar muito dinâmico. Um fórum online pode estar em um URL específico em um dia e desaparecer no dia seguinte. Os esquemas de nomenclatura e endereço na Deep Web mudam frequentemente. Isso significa que as informações que coletamos há duas semanas não são mais relevantes hoje. Isso tem implicações na prova do crime. Considerando o prazo em que os casos criminais são julgados, as forças de segurança devem ser capazes de documentar rigorosamente qualquer atividade criminosa online por meio de capturas de tela com carimbo de data / hora para evitar que os casos se tornem inválidos.<sup>145</sup>

Em contrapartida, e para o bem comum, as ferramentas de anonimato que os criminosos dispõem, já se sabe, não são totalmente eficazes, e já há casos de investigações bem sucedidas que foram realizadas no ambiente da *Dark Web*.

Assim, engana-se o usuário que acredita que, navegando através da rede TOR, terá um anonimato absoluto.

Estudos publicados comprovam a eficácia de metodologias próprias de coleta de informação do fluxo dos dados trafegados pela *deep web*. Afirmam ainda terem conseguido o acesso a alguns dos pontos de troca de tráfego na Internet, o que seria o bastante para monitorar os caminhos da rede a partir dos nós da Tor até servidores destino.<sup>146</sup>

As autoridades policiais estão, portanto, se aprimorando, e o desenvolvimento de ferramentas que permitam a identificação de usuários, aliado ao cometimento de falhas por parte dos criminosos durante a navegação, têm permitido o êxito em diversas investigações cibernéticas.

<sup>145</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web**. Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 38. Texto original: *Law enforcement agencies already face several existing challenges when it comes to international crime on the Surface Web. With regard to the Deep Web, three additional aspects can make law enforcement even more problematic.*

- *Encryption: Everything in the Deep or Dark Web is encrypted. That means the criminals in it are much more aware about being trapped or monitored. Encryption is their very first countermeasure to evade detection.*

- *Attribution: It's extremely difficult to determine attribution. Everything happens on .onion domains. Routing to these domains is also unclear.*

- *Fluctuation: The Deep Web is a very dynamic place. An online forum can be at a specific URL one day and gone the next. The naming and address schemes in the Deep Web often change. This means that the information we harvested two weeks ago is no longer relevant today. This has implications in proving crime. Considering the time frame in which criminal cases are tried, law enforces must be able to rigorously document any criminal online activity via time-stamped screenshots in order to prevent cases from becoming invalid.*

<sup>146</sup> BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELI, Guilherme. **Investigação digital em fontes abertas**. 2. ed. Rio de Janeiro: Brasport, 2017, p. 212.

### 2.2.2.2 Bitcoin e Dark Web

A contraprestação dos produtos comercializados e dos serviços prestados na *Dark Web* é efetivada costumeiramente através do *Bitcoin*, tratando-se de uma criptomoeda descentralizada, e que é utilizada como uma espécie de dinheiro eletrônico.

O serviço de *Bitcoin* é um produto mundialmente aceito, descentralizado, e não regulamentado ou fiscalizado por qualquer rede de bancos, instituições financeiras ou servidores governamentais. Ainda, esta moeda guarda a especificidade de não ser gerenciada por um grande servidor, e essa atribuição fica a cargo de uma complexa rede denominada de “mineradores”, que, através de serviços P2P (*player to player* ou *peer to peer*), ficam responsáveis pelo gerenciamento e pela validação de todas as transações realizadas na *internet*.

Qualquer pessoa hoje pode adquirir uma carteira de *Bitcoins* e realizar transações na rede. Para se ter uma ideia, existem corretoras especializadas na sua comercialização, e inclusive bolsas de valores ao redor do mundo já a comercializa.

Em valores atuais em Reais, um *Bitcoin* equivale a R\$ 96.401,00<sup>147</sup>, o que demonstra o real interesse por parte das pessoas neste tipo de tecnologia, já que em junho de 2016 um *Bitcoin* era comercializado por R\$ 2.523,00.

Para realizar qualquer compra virtual em que a moeda balizada seja o bitcoin, é preciso que as duas “carteiras” da transação sejam conectadas. Essa conexão é criptografada e as informações da negociação são incluídas na cadeia de blocos de transações realizadas. Sua validação é realizada pelos mineradores, que confirmam sua autenticidade. Ainda que a transação seja pública, a identidade dos donos da carteira é mantida em segredo, o que torna seu rastreamento impossível.<sup>148</sup>

As transações realizadas em *Bitcoins*, apesar da prevalência do anonimato das partes envolvidas, são públicas, o que permite, de certa maneira, que uma transação objeto de uma investigação seja rastreada, e a depender do nível de segurança que foi adotada na transação, expô-la aos investigadores, que poderão identificar os usuários da referida transação.

Pensando em burlar essa possibilidade de êxito, na *Dark Web* já é possível encontrar ferramentas que tornam a transação comercial em *Bitcoins* ainda mais segura no tocante a publicidade da negociação, possibilitando até, caso queira o

---

<sup>147</sup> Cotação de um *Bitcoin*. Disponível em: <https://www.mercadobitcoin.com.br/>. Acesso em: 19 nov. 2020.

<sup>148</sup> BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELI, Guilherme. **Investigação digital em fontes abertas**. 2. ed. Rio de Janeiro: Brasport, 2017, p. 212.

proprietário do *Bitcoin*, transformar a moeda digital em moeda corrente de seu país, estabelecendo uma espécie de câmbio ilegal, ocorrendo a lavagem do dinheiro. Sobre o *Bitcoin*, Ciancaglili, Balduzzi, McArdle e Rosler ensinam:

Por si só, o Bitcoin é uma moeda projetada com o anonimato em mente. Como resultado, é frequentemente usada na compra de bens e serviços ilegais. Embora todas as transações de Bitcoin sejam anônimas (contanto que você não vincule o código da carteira à sua identidade real), elas são totalmente públicas. Rastrear o dinheiro conforme ele se move pelo sistema é, portanto, viável, embora bastante difícil. Como resultado, vários serviços que adicionam mais anonimato ao sistema surgiram, tornando a moeda eletrônica ainda mais difícil de rastrear.<sup>149</sup>

Algumas ferramentas permitem que o usuário potencialize ainda mais o anonimato ao realizar uma transação na *Dark Web* através de *Bitcoins*<sup>150</sup>. A promessa é de total segurança, e a garantia é que não haverá invasão do sistema por pessoas estranhas, e que venham colocar em risco a identidade de seus usuários.

Não bastasse a problemática causada pelo anonimato daqueles que fazem uso do TOR em ambiente de *Dark Web*, os criminosos ainda lançam mão do uso do *Bitcoin* como meio de negociação nas atividades ilícitas, e diante da impossibilidade de rastrear a utilização deste tipo de moeda, depara-se aqui as autoridades com mais um obstáculo à investigação cibernética.

### 2.2.2.3 Criminalidade na *Dark Web*

Com o objetivo de entender melhor a navegação na *Dark Web*, a empresa Trend Micro, através de sua equipe de especialistas, desenvolveu um sistema de análise que coletou informações importantes tais como, por exemplo, o conteúdo das páginas acessadas, mesmo que o acesso seja feito através da ferramenta TOR. Através deste sistema, foi possível apurar alguns dados relevantes, dentre as quais, que o principal idioma utilizado nos domínios dentro da *Dark Web* é o inglês, porém a maioria dos sites disponíveis estão no idioma russo. Assim descreve o relatório: “Em termos de número bruto de domínios, o inglês foi o principal idioma escolhido por pelo

<sup>149</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 22. Texto original: *On its own, Bitcoin is a currency designed with anonymity in mind. As a result, it's frequently used when purchasing illegal goods and services. While all Bitcoin transactions are anonymous (as long as you don't link your wallet code to your real identity), they are fully public. Tracking money as it moves through the system is thus doable, albeit quite difficult. As a result, a number of services that add further anonymity to the system have surfaced, making the electronic currency even more difficult to track.*

<sup>150</sup> Imagem 02 do Anexo A, p. 124.

menos 2.154 sites dos 3.454 domínios explorados com sucesso. Isso representa cerca de 62% do número total de sites. Em seguida, veio o russo (228 domínios), depois o francês (189 domínios)".<sup>151</sup> E mais: Olhando para a distribuição de idiomas com base no número de URLs, o russo venceu o inglês porque, apesar de ter menos sites, o número de sites que usavam o russo era maior.<sup>152</sup><sup>153</sup>

Como a maioria dos sites existentes são divulgados no idioma russo, depara-se aqui a investigação com mais um obstáculo na busca pela colheita de prova nesse ambiente, pois em se tratando de um idioma bastante complexo, intérpretes deverão ser utilizados na investigação.

O sistema analisou ainda os principais sites de comércio existentes na *Dark Web*, e constatou que a maioria dos acessos são em busca da aquisição de drogas ilícitas, seguida por medicamentos, muitos deles controlados, e vendidos obviamente sem prescrição médica.<sup>154</sup>

Uma análise dos 15 principais fornecedores em todos os mercados mostrou que as drogas leves eram os produtos mais trocados na Deep Web. Em seguida, vieram produtos farmacêuticos como Ritalina e Xanax, drogas pesadas e até jogos piratas e contas online. Esses dados corroboram a ideia de que a maioria dos usuários da Deep Web, pelo menos aqueles que frequentam os principais mercados, vão lá para comprar drogas ilícitas.<sup>155</sup>

Constata-se, portanto, que a maior parte do comércio exercido na *Dark Web* envolve o tráfico de drogas, tanto lícitas quanto ilícitas. A disponibilidade de narcóticos ilegais varia muito na *Deep Web*, e alguns sites vendem de tudo, desde cigarros contrabandeados, até *cannabis* e cocaína.<sup>156</sup>

<sup>151</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 9. Texto original: *In terms of raw number of domains, English was the main language of choice by at least 2,154 sites out of the 3,454 successfully scouted domains. That roughly makes up 62% of the total number of sites. This was followed by Russian (228 domains) then French (189 domains).*

<sup>152</sup> *ibidem*, p. 10. Texto original: *Looking at the language distribution based on number of URLs, Russian beat English because, despite having fewer sites, the number of sites that used Russian was bigger.*

<sup>153</sup> Imagem 03 do Anexo A, p. 125.

<sup>154</sup> Imagem 04 do Anexo A, p. 126.

<sup>155</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 10. Texto original: *An analysis of the top 15 vendors across all marketplaces showed that light drugs were the most-exchanged goods in the Deep Web. This was followed by pharmaceutical products like Ritalin and Xanax, hard drugs, and even pirated games and online accounts. This data backed up the idea that a majority of Deep Web users – at least those who frequent the top marketplaces – go there to purchase illicit drugs.*

<sup>156</sup> Imagem 05 do Anexo A, p. 127.

Há ainda à disposição dos usuários da *Dark Web* uma ferramenta de busca denominada *Grams*, que é usada exclusivamente para localizar fornecedores de drogas naquele ambiente.<sup>157</sup>

A procura por drogas na *Dark Web* é tão intensa, que aparentemente não será suficiente identificar os canais de vendas e evitar sua veiculação. Constata-se que, como no ambiente físico, a procura pelas drogas parece não diminuir, e se de um lado existem os compradores em números aparentemente cada vez mais crescentes, do outro há os vendedores, procurando atender as necessidades de tal demanda. Caso o site seja identificado e retirado do ar, outro com as mesmas características infelizmente tomará lugar e retomará a comercialização ilegal.

Outros crimes bastante comuns que são praticados na *Dark Web*, além do tráfico de drogas, são a comercialização de dados bancários, de contas de *PayPal*<sup>158</sup>, de cartões de crédito<sup>159</sup>, além da falsificação de documentos diversos, como passaportes e até cidadania de países diversos.<sup>160</sup>

Passaportes, documentos de extremo valor não somente por identificar uma pessoa em serviços de imigração no mundo todo, mas também por permitir a possibilidade de abertura de contas em bancos, obtenção de empréstimos, aquisição de propriedades, etc., também são objetos de falsificações na *Dark Web*<sup>161</sup>, e por preços médios de 500 (quinhentos) Euros.<sup>162</sup>

Finalizando este tópico, e não esgotando a relação dos inúmeros crimes que são praticados na *Dark Web*, outro serviço que também é encontrado neste ambiente é a contratação de assassinos de aluguel. Os preços ofertados variam de acordo com o tipo de lesão que o contratante deseja ocasionar à vítima, cujos menores valores se referem a uma surra, passando pela inutilização de membros do corpo, chegando até a morte, cujos preços serão mais elevados.<sup>163</sup> A posição social e a profissão são fatores que serão levados em conta para precificar os serviços.

Não há evidências de que a oferta deste tipo de serviço seja real, pois até então não se conhece a relação existente entre uma investigação de assassinato e a contratação deste tipo de serviço na *Dark Web*. O próprio site não divulga qualquer tipo

---

<sup>157</sup> Imagem 06 do Anexo A, p. 128.

<sup>158</sup> Imagem 07 do Anexo A, p. 129.

<sup>159</sup> Imagem 08 do Anexo A, p. 130.

<sup>160</sup> Imagem 09 do Anexo A, p. 131.

<sup>161</sup> Imagem 10 do Anexo A, p. 132.

<sup>162</sup> Imagem 11 do Anexo A, p. 133.

<sup>163</sup> Imagem 12 do Anexo A, p. 134.



de prova de que os serviços foram executados, sob o pretexto de preservar a segurança de seus contratantes e também dos executores.

Mesmo não sendo disponibilizadas provas, o site divulga que o pagamento integral somente será realizado quando o serviço for concluído, o que será provado exclusivamente ao contratante. Fato é que, apesar da dúvida existente quanto a veracidade das informações constantes nesses tipos de sites, não se pode descartar a possibilidade de serem reais.

### **3 – Instrumentos aditivos ao enfrentamento dos crimes cibernéticos**

O terceiro e último capítulo deste trabalho abará alguns aspectos relacionados à três instrumentos aditivos de enfrentamento dos crimes cibernéticos, que ao serem adotados pelo Estado brasileiro contribuirão para minimizar os danos causados pela incidência cada vez maior da criminalidade no ambiente digital. O primeiro deles trata da educação digital através de processos educacionais e a adoção pelo Estado de políticas públicas de conscientização, visando aprimorar os conhecimentos dos cidadãos e cidadãs no uso da tecnologia.

O segundo instrumento aditivo trata da reavaliação e adequação legislativa no sentido de melhor adequar as condutas ilícitas praticadas na *internet* aos tipos penais já existentes, além da criminalização de condutas ainda não previstas no ordenamento jurídico penal brasileiro, demonstrando-se a importância do estabelecimento de uma legislação robusta e eficiente com o objetivo de contribuir para a obtenção de melhores resultados nas investigações nos crimes cibernéticos e na sua persecução penal.

Encerra-se o capítulo com o estudo do terceiro e último instrumento aditivo ao enfrentamento dos crimes cibernéticos, a Convenção de Budapeste, demonstrando-se a importância da adesão do Brasil à Convenção para a obtenção dos diversos benefícios por ela trazidos, aprimorando por consequência o enfrentamento à criminalidade cibernética em nosso país.

#### **3.1 Educação digital: políticas públicas para o uso responsável da *internet***

Indiscutivelmente a educação, como direito fundamental, promove mudanças significativas no desenvolvimento pessoal de cada cidadão e cidadã e consequentemente no desenvolvimento de uma nação. Sua importância ultrapassa a satisfação de melhores oportunidades de emprego e sucesso profissional, alcançando o aprimoramento dos aspectos social e cultural de cada indivíduo, contribuindo para uma melhor compreensão do ambiente em que está inserido e estabelecendo fundamentalmente seu desenvolvimento crítico.

A educação é um processo permanente, e ao longo da vida cada indivíduo tem a oportunidade de experimentar o conhecimento como forma de lapidar seu

intelecto, tornando-se numa pessoa mais bem evoluída. Paulo Freire, ao descrever seu posicionamento sobre a educação, ensina que:

É na inconclusão do ser, que se sabe, como tal, que se funda a educação como processo permanente. Mulheres e homens se tornaram educáveis na medida em que se reconheceram inacabados. Não foi a educação que fez mulheres e homens educáveis, mas a consciência de sua inconclusão é que gerou sua educabilidade.<sup>164</sup>

Neste contexto da educação, admitindo-se que as pessoas inacabadas em seu processo de aprendizado e diante do surgimento da chamada sociedade da informação, seria imprudente deixar de admitir que se faz necessário um conjunto de ações educacionais que permita a todos obter conhecimentos sobre os aspectos relacionados à era digital. O Brasil é um dos países com mais acessos à internet no mundo, e como já descrito no primeiro capítulo deste trabalho, o relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento<sup>165</sup> (UNCTAD) emitido no ano de 2017, coloca o país em quarto lugar no *ranking* do número de usuários de *internet*, ficando atrás somente dos Estados Unidos, Índia e China.

Problemas relacionados à segurança e à privacidade dos usuários são muito comuns quando a tecnologia é utilizada sem uma base mínima de conhecimento à respeito, de forma indiscriminada, e sem qualquer preocupação com requisitos mínimos de cuidado.

Diante de todos os benefícios trazidos pela tecnologia que está inserida nos meios de comunicação contemporâneos e que são utilizados pelas pessoas cotidianamente, acaba por demandar melhores conhecimentos sobre o uso adequado e seguro das ferramentas tecnológicas. Não basta fazer uso de meios tecnológicos em métodos de ensino ou facilitar à população a aquisição de aparelhos eletrônicos com acesso à *internet*. O grande desafio consiste em ensinar como fazer uso da tecnologia inserida nesses aparelhos, com bom senso e ética, de modo que minimize os danos ocasionados por ações pelo mau uso e práticas criminosas na rede. É de suma importância que o Estado estabeleça conteúdos educacionais voltados para a capacitação do uso da tecnologia e crie políticas públicas de conscientização com o objetivo de demonstrar a todos a necessidade de ter-se discernimento para assimilar

---

<sup>164</sup> FREIRE, Paulo. **Pedagogia da autonomia: saberes necessários à prática educativa**. 63. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2020, p.57.

<sup>165</sup> ONU. **UNCTAD 2017 – United nations conference on trade and development**. Disponível em: [https://unctad.org/en/PublicationsLibrary/wir2017\\_en.pdf](https://unctad.org/en/PublicationsLibrary/wir2017_en.pdf). Acesso em 25 jul. 2019.

as informações disponíveis na *internet* e tirar o melhor proveito da conectividade para o desenvolvimento de suas capacidades.

Neste sentido, em relação ao bom senso, Paulo Freire ensina que:

O exercício ou a educação do bom-senso vai superando o que há nele de instintivo na avaliação que fazemos dos fatos e dos acontecimentos em que nos envolvemos. Se o bom-senso, na avaliação moral que faço de algo não basta para orientar ou fundar minhas táticas de luta, tem, indiscutivelmente, importante papel na minha tomada de posição, a que não pode faltar a ética, em face do que devo fazer.<sup>166</sup>

Não se trata simplesmente da transmissão do conhecimento de forma técnica, e o processo educacional deve abordar inclusive aspectos relacionados à ética, como já mencionado neste trabalho. Somente assim haverá um processo de conscientização que permita ao usuário da *internet* perceber os riscos decorrentes do mau uso da tecnologia e os danos que poderão ser ocasionados em decorrência de sua utilização indiscriminada e sem o estabelecimento de qualquer critério.

Freire<sup>167</sup> ainda ensina que não é possível imaginar os seres humanos distante da ética, quanto mais fora dela, pois isso significaria uma transgressão, onde a transformação do processo educacional em treinamento puramente técnico deixa de contemplar o que há de fundamentalmente humano no exercício da educação, o seu caráter formador. Aquele que ensina, e que respeita a natureza do ser humano, estará respeitando a formação moral daquele que aprende.

O usuário da *internet* deve, portanto, ter seus conhecimentos aprimorados de modo que o uso que se faz da tecnologia seja cada dia mais maduro e consciente, proporcionando uma relação afável com os demais usuários da rede. Interessantes são os ensinamentos de Freire ao tratar do processo educacional, estabelecendo a seguinte metáfora em relação ao aprimoramento do saber.

O ato de cozinhar, por exemplo, supõe alguns saberes concernentes ao uso do fogão, como acendê-lo, como equilibrar para mais, para menos, a chama, como lidar com certos riscos, mesmo remotos, de incêndio, como harmonizar os diferentes temperos numa síntese gostosa e atraente. A prática de cozinhar vai preparando o novato, ratificando alguns daqueles saberes, retificando outros, e vai possibilitando que ele vire cozinheiro. A prática de velejar coloca a necessidade de saberes fundantes como o de domínio do barco, das partes que o compõem e da função de cada uma delas, como o conhecimento dos ventos, de sua força, de sua direção, os ventos e as velas, a posição das velas, o papel do motor e da combinação entre motor e velas.

---

<sup>166</sup> FREIRE, Paulo. **Pedagogia da autonomia: saberes necessários à prática educativa**. 63. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2020, p.61.

<sup>167</sup> *ibidem*, p.34.

Na prática de velejar se confirmam, se modificam ou se ampliam esses saberes.<sup>168</sup>

A educação tem um papel fundamental na formação das pessoas desde a mais tenra idade. Oportunizar à criança o acesso à educação permite estimular seus conhecimentos para obter um melhor convívio social, estabelecer o respeito ao próximo como sendo a regra, gerar responsabilidades e fundamentalmente exercer a cidadania e por consequência tornar-se um bom cidadão.

A curiosidade que é gerada, principalmente nas crianças, ao serem apresentadas à tecnologia, deve ser utilizada no processo educacional em proveito das próprias crianças, favorecendo a implementação de um processo de educação digital que leve aos futuros precoces usuários da *internet* a serem inseridos no mundo digital mais bem preparados para os desafios que surgirão pela frente.

Neste contexto Freire destaca a importância da curiosidade no sentido de contribuir para o processo educacional, ensinando que:

O exercício da curiosidade convoca a imaginação, a intuição, as emoções, a capacidade de conjecturar, de comparar, na busca da perfilização do objeto do achado de sua razão de ser. Um ruído, por exemplo, pode provocar minha curiosidade. Observo o espaço onde parece que se está verificando. Aguço o ouvido. Procuo comparar com outro ruído cuja razão de ser já conheço. Investigo melhor o espaço. Admito hipóteses várias em torno da possível origem do ruído. Elimino algumas até que chego a sua explicação.<sup>169</sup>

Portanto, a curiosidade gerada nas crianças pelas novas formas de comunicação tecnológicas deve servir de estopim para proporcionar conhecimentos mais apurados sobre o assunto, permitindo o desfrute do que a tecnologia tem de melhor a oferecer, minimizando riscos aos próprios usuários, e por consequência colaborando para a redução da criminalidade cibernética.

Freire ainda destaca o papel da escola neste contexto da curiosidade, ensinando que:

Uma das tarefas essenciais da escola, como centro de produção sistemática de conhecimento, é trabalhar criticamente a inteligibilidade das coisas e dos fatos e a sua comunicabilidade. É imprescindível, portanto, que a escola instigue constantemente a curiosidade do educando em vez de amaciá-la ou domesticá-la. É preciso mostrar ao educando que eu uso ingênuo da curiosidade altera a sua capacidade de achar e obstaculiza a exatidão do achado. É preciso por outro lado, e sobretudo, que o educando vá assumindo o papel de sujeito da produção de sua inteligência do mundo e não apenas o de receptor da que lhe seja transferida pelo professor. Quanto mais me

---

<sup>168</sup> FREIRE, Paulo. **Pedagogia da autonomia: saberes necessários à prática educativa**. 63. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2020, p.23.

<sup>169</sup> *ibidem*, p.85.

torno capaz de me afirmar como sujeito que pode conhecer, tanto melhor desempenho minha aptidão para fazê-lo.<sup>170</sup>

A maturidade alcançada através do processo educacional, seja na formação escolar, no seio da família e ainda no convívio social, permite a todos discernir melhor sobre todos os aspectos da vida em sociedade, corroborando para o aprimoramento das habilidades e competências. O desenvolvimento do saber decorre do empenho do educador de, aproveitando-se do estado de curiosidade que surge em decorrências do uso da tecnologia, obtém melhores resultados na sua tarefa de ensinar. Não se trata somente de transferir o conhecimento de forma técnica e “fria”, como Paulo Freire chama de “método bancário” de ensinar. Neste sentido, Freire ensina que:

O educador democrático não pode negar-se o dever de, na sua prática docente, reforçar a capacidade crítica do educando, sua curiosidade, sua insubmissão. Uma de suas tarefas primordiais é trabalhar com os educandos a rigorosidade metódica com que devem se “aproximar” dos objetos cognoscíveis. E esta rigorosidade metódica não tem nada a ver com o discurso “bancário” meramente transferidor do perfil do objeto ou do conteúdo. É exatamente neste sentido que ensinar não se esgota no “tratamento” do objeto ou do conteúdo, superficialmente feito, mas se alonga à produção das condições em que aprender criticamente é possível. E essas condições implicam ou exigem a presença de educadores e de educandos criadores, instigadores, inquietos, rigorosamente curiosos, humildes e persistentes. Faz parte das condições em que aprender criticamente é possível a pressuposição por parte dos educandos de que o educador já teve ou continua tendo experiência da produção de certos saberes e que estes não podem a eles, os educandos, ser simplesmente transferidos. Pelo contrário, nas condições de verdadeira aprendizagem os educandos vão se transformando em reais sujeitos de construção e da reconstrução do saber ensinado, ao lado do educador, igualmente sujeito do processo. Só assim podemos falar realmente de saber ensinado, em que o objeto ensinado é aprendido na sua razão de ser e, portanto, apreendido pelos educandos.<sup>171</sup>

Além disso, a educação formal, aquela promovida pelo Estado através dos bancos escolares, onde o conhecimento é transmitido por um educador, não é a única forma de educar. Deve-se levar em consideração para a formação do indivíduo a educação que é proporcionada através da informalidade, por meio do convívio social e com a família, e que ocorre de forma espontânea.

No âmbito da educação informal, muito pode-se contribuir para aprimorar os conhecimentos das pessoas acerca da tecnologia. A troca de experiências já vivenciadas, por exemplo, é uma excelente forma de compartilhar o conhecimento, seja no ambiente de trabalho, nos encontros sociais ou ainda no seio familiar.

---

<sup>170</sup> FREIRE, Paulo. **Pedagogia da autonomia: saberes necessários à prática educativa**. 63. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2020, p.121.

<sup>171</sup> *ibidem*, p.28.

Como visto, a educação digital é fundamental para minimizar os riscos inerentes à navegação na internet. A conscientização e ampliação de conhecimentos sobre os assuntos relacionados à tecnologia certamente poderão contribuir para minimizar os danos causados pela criminalidade cibernética. O Estado deve atentar-se para a importância do estabelecimento de políticas públicas voltadas para a finalidade da educação digital, além é claro de inserir conteúdos programáticos nas escolas que irão contribuir para que o aluno desde os primeiros anos nos bancos escolares possam ter acesso e essa espécie de conhecimento.

Por mais que os dados fornecidos pelo Estado indiquem que a educação no país tem avançado nos últimos anos, o que se observa é que ainda é deficitária, e é notório que ainda há muito o que melhorar, não somente no processo educacional de conteúdo tradicional, mas também naquele voltado ao uso da tecnologia.

### **3.2 Processo legislativo: reavaliação e adequação de condutas e tipos penais**

No processo de enfrentamento aos crimes cibernéticos não é possível deixar de contemplar a reavaliação e adequação dos tipos penais para melhor enquadrar as condutas delitivas praticadas na *internet*. Para se obter melhores resultados nas investigações cibernéticas e na persecução penal, e por consequência o Estado ser mais efetivo ao prestar sua tutela, tanto o Código Penal quanto o Código de Processo Penal deverão passar por alterações visando maior efetividade das leis. Como ensinam Jesus e Milagre:

Em se tratando de crimes informáticos, deve-se registrar que as características da Internet não permitiram tão somente o desenvolvimento da comunicação, mas serviram de ambiente para o crescimento de crimes de informática, estes amparados pela sensação de anonimato e pouca possibilidade de punição, considerando que até recentemente tudo que o Brasil tinha em termos legislativos no que diz respeito a crimes informáticos era a Lei nº 9.983/2000, que poucos artigos acrescentou ao Código Penal, aplicáveis, via de regra, a funcionários públicos. No mundo, o crime virtual já é o terceiro em prejuízo, apenas atrás das drogas e da falsificação.<sup>172</sup>

Diante da evolução tecnológica e do aprimoramento dos mecanismos utilizados pelos criminosos para a prática delitiva no ambiente cibernético, observa-se uma lacuna legislativa no ordenamento jurídico penal brasileiro, e que acaba por

---

<sup>172</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 68.

permitir a maior incidência dos crimes cibernéticos. Há de se avaliar uma alternativa no sentido de as casas legislativas dedicarem maiores esforços para adequar a legislação à nova realidade mundial.

Neste sentido Malaquias ensina que:

Enquanto a casa legislativa não se posiciona, desgastando-se perante a opinião pública em intermináveis debates de emendas legislativas inócuas e ineficazes, o lapso temporal se amplia dramaticamente e os fatos sociais se alternam entre os avanços tecnológicos e a criatividade incessante dos criminosos cibernéticos, decorrente da tutela jurídica deficitária, restando aos operadores do direito e aos profissionais da ciência da informação considerar como fonte de uniformização normativa as pequenas reformas processuais que modificaram pontualmente certos tipos penais e, paralelamente, efetuam diversas tentativas de disponibilização dos preceitos contidos nos tratados e convenções internacionais que dispõem sobre o mencionado tema por via oblíqua, em pontuais modificações da norma adjetiva.<sup>173</sup>

Jesus e Milagre<sup>174</sup> ainda ressaltam que o processo legislativo muito provavelmente não acompanhará os avanços na área da tecnologia, não significando que os profissionais do direito devem se manter omissos, aguardando providências do poder legislativo na elaboração de leis que atendam as demandas geradas pelos crimes cibernéticos. Segundo os autores, o Direito deve estar sempre atualizado visando a proteção das pessoas lesadas, aplicando a legislação vigente e concebendo tipos penais específicos para as condutas praticadas na *internet*.

Diante do modo como hoje é estabelecido o enfrentamento aos crimes cibernéticos, acaba por gerar insegurança dos cidadãos e cidadãs que a cada dia mais fazem uso de todos os benefícios trazidos pela tecnologia e que está inserida nas formas de se relacionarem com o mundo, e que em virtude da própria tecnologia de que fazem uso, se veem envolvidos na condição de vítimas em ilícitos no ambiente virtual, e o grande beneficiário da lacuna legislativa existente é o próprio criminoso, que raramente é identificado e punido pelos crimes cometidos. Malaquias ainda ensina que:

Apesar de não haver legislação coesa que possa abordar, contemplar e reprimir adequadamente os crimes cibernéticos em sua totalidade, os fenômenos sociais e jurídicos têm obrigado os operadores do direito a lançarem mão de imputação difusa e deficiente, dando margem à defesa do acusado que se fortalece com as falhas constitutivas insurgentes aderidas como resistente amálgama no tipo penal, envenenando a responsabilidade

---

<sup>173</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 252.

<sup>174</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 25.



civil e penal, consolidando a impunidade e gerando o caos e a anarquia no espaço cibernético.<sup>175</sup>

O que se constata é que deve haver uma evolução do processo legislativo, acompanhando toda evolução tecnológica, e de modo que atenda as novas demandas no mundo moderno e inserido nos processos que envolvem a tecnologia. Além das inúmeras demandas já existentes da sociedade, os legisladores deverão estar atentos para essa evolução da criminalidade e melhor adequar as leis brasileiras para essa finalidade. Sobre a relevância do processo de transformação das leis e de todos os aspectos jurídicos que envolvem a evolução tecnológica, Malaquias ensina que:

A metamorfose da ciência jurídica é um de seus fundamentos mais especiais e sua constante transformação consolida a nobreza de seu objeto que agora, além de acompanhar as modificações sociais no espaço delimitado pelo território tradicional, surge o desafio de controlar o espaço cibernético, tendo em vista que as diversas atividades humanas migram velozmente para o ambiente intangível, virtual, constituindo-se modernamente na sociedade cibernética.<sup>176</sup>

A adequação legislativa para o melhor enfrentamento dos crimes cibernéticos já tem ocorrido em diferentes países, e tanto o direito material penal quanto o direito processual já passaram por alterações nesses países visando compatibilizar as demandas originadas pela criminalidade no ambiente virtual.

Em Portugal, a Lei nº 109/2009<sup>177</sup>, conhecida como a Lei do Cibercrime, adaptou o direito interno português à Convenção de Budapeste, abarcando disposições penais materiais e disposições processuais. Quanto ao direito material, o artigo 3º tipifica o crime de falsidade informática, estabelecendo que aquele que, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, será punido com pena de prisão de até 5 anos ou multa de 120 a 600 dias.

---

<sup>175</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 251.

<sup>176</sup> *ibidem*, p. 252.

<sup>177</sup> PORTUGAL. **Lei nº 109 de 15 de setembro de 2009**. Lei do Cibercrime. Disponível em: [http://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=1137&tabela=leis&ficha=1&pagina=1&so\\_miolo=S](http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis&ficha=1&pagina=1&so_miolo=S). Acesso em: 04 nov. 2020.

Quando as ações descritas no artigo 3º incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena será de 1 a 5 anos de prisão.

O número 3 do mesmo artigo ainda prevê que aquele que, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no número 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número 2, será punido com as penas previstas num e noutra número, respectivamente.

Há ainda a previsão de o agente ser punido por importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no número 2, com pena de prisão de 1 a 5 anos. E por fim, o artigo 3º traz a previsão de que se os fatos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena será de prisão de 2 a 5 anos.

A mesma lei portuguesa, além de especificar as condutas relativas à falsidade informática como descrito acima, ainda tipifica as condutas de dano relativo a programas e outros dados informáticos, sabotagem informática, acesso ilegítimo, interceptação ilegítima, reprodução ilegítima de programa protegido, prevendo ainda a possibilidade das pessoas jurídicas serem responsabilizadas pelos crimes previstos na lei.

Já no tocante aos aspectos processuais, a Lei 109/2009, a partir do artigo 11º estabelece uma série de procedimentos que buscam aperfeiçoar a persecução penal naquele país, como a preservação de dados para a produção de provas, revelação de dados de tráfego, apresentação ou concessão de acesso aos dados, pesquisa de dados informáticos, apreensão de dados informáticos, apreensão de correio eletrónico e registros de comunicações, interceptação de comunicações e ações encobertas. Por fim, no Capítulo IV da referida lei, há a previsão de todos os aspectos relacionados à cooperação internacional no enfrentamento aos crimes cibernéticos.

Na Itália, conforme descreve Malaquias<sup>178</sup>, também há a disposição de normas modernas, como é o caso da lei processual penal daquele país, que trata do objeto da prova no Título I, do art. 187 ao art. 193. No Título II, do art. 194 ao art. 243, preceitua sobre os meios de prova, sendo que, no Título III, do art. 244 ao art. 271, estabelece procedimentos relevantes para tratar sobre os meios de obtenção de prova. Já no Capítulo IV preceitua sobre as interceptações das conversações ou comunicações, inclusive na área de informática e telemática.

Na Espanha, o Código Penal<sup>179</sup> daquele país prevê diversas condutas relacionadas aos crimes cibernéticos. No Título X, Capítulo I, há a previsão dos delitos contra a intimidade e que é praticado na *internet*. No Capítulo VI estão previstos os crimes de fraudes praticadas por meio de recursos de informática. No artigo 256 está prevista a conduta do uso indevido de dispositivo de telecomunicações sem o consentimento do proprietário. Já no Capítulo IX estão previstos os crimes de danos, e no artigo 264 é punida a conduta daquele que, por qualquer meio, sem autorização e de forma grave, apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis dados, programas de computador ou documentos eletrônicos externos, quando o resultado produzido for grave. No Capítulo XI há ainda a previsão dos crimes contra a propriedade intelectual e industrial previstos nos artigos 270 e seguintes.

Malaquias<sup>180</sup> ressalta que nos Estados Unidos da América a legislação é bastante severa quanto aos crimes cometidos no ambiente virtual, e até mesmo uma infração que seria considerada de menor potencial ofensivo em outros países, lá é tratada de forma severa, como por exemplo o *spamming*<sup>181</sup>. Segundo o sistema jurídico americano, aquele que for considerado *spamer* será condenado na área cível a pagar severas multas que variam entre US\$ 500 (quinhentos dólares americanos) e US\$ 25 mil (vinte e cinco mil dólares americanos), além de ser responsabilizado na esfera penal pelos atos praticados.

---

<sup>178</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 250.

<sup>179</sup> ESPANHA. **Código Penal Espanhol**. Disponível em: [https://oig.cepal.org/sites/default/files/2003\\_esp\\_codpenal-actualizado2011.pdf](https://oig.cepal.org/sites/default/files/2003_esp_codpenal-actualizado2011.pdf). Acesso em: 04 nov. 2020.

<sup>180</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 250.

<sup>181</sup> *Spaming* é o nome que se dá a atividade ilícita de envio de e-mail, geralmente com conteúdos de *marketing*, e que ao serem abertos pelos seus destinatários, instala em seus dispositivos um vírus ou outro código malicioso.

Como é possível constatar do direito comparado, os países estrangeiros estão um passo à frente quando o tema é a alteração legislativa para melhor adequar o enfrentamento dos crimes cibernéticos. O Brasil está, e muito, atrasado em termos de contar com uma legislação penal informática eficiente e capaz de dar uma resposta compatível com os crimes praticados. Jesus e Milagre ainda ensinam que:

Questionou-se muito da necessidade de uma lei específica para tanto. Para muitos autores o foco do Direito Penal é a proteção de bens jurídicos individuais, não sendo coerente a aplicação penal de interesses supraindividuais. Em tese, a conduta delitiva deveria lesionar bens pessoais e não direitos. Na era digital, porém, acentua-se a tutela penal dos direitos difusos. Passamos a considerar o objetivo da Lei Penal com o escopo de proteger a segurança e possibilitar a vida da sociedade digital.<sup>182</sup>

Importante ressaltar que um conjunto de normas jurídicas bem estruturadas será instrumento fundamental para o enfrentamento dos crimes cibernéticos. Para tanto, torna-se imprescindível promover mudanças de âmbito legislativo e nas atividades jurisdicionais, de modo que o tema cibercriminalidade seja efetivamente discutido e permita ao Estado prestar sua tutela de forma mais efetiva, não somente contribuindo para a evolução do Direito, mas proporcionando melhores condições para aplicação da lei a todos aqueles que direta ou indiretamente somam esforços para minimizar os males causados pela criminalidade no ambiente virtual.

### **3.3 Convenção de Budapeste: a adesão do Brasil como alternativa ao enfrentamento dos crimes cibernéticos**

Visando estabelecer uma regulamentação comum e ações conjuntas entre países para o enfrentamento dos crimes cibernéticos, no ano de 2001 foi firmado pelo Conselho da Europa a Convenção do Cibercrime,<sup>183</sup> que visa tipificar diversas condutas ilícitas praticadas na *internet*, além de estabelecer procedimentos processuais comuns entre os países signatários, possibilitando ainda a cooperação internacional para o sucesso das investigações dos crimes que tenham como uma de suas características a transnacionalidade.

Neste sentido, Roberto Antônio Darós Malaquias ensina que:

---

<sup>182</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 69.

<sup>183</sup> CONVENÇÃO SOBRE O CIBERCRIME. **Convenção de Budapeste. 2001**. Disponível em [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf). Acesso em: 14 out. 2020.

A comunidade europeia encontra-se num estágio mais avançado que o restante das nações desenvolvidas no que se refere à normatização do espaço cibernético. O Conselho da Europa adotou a Convenção de Budapeste contra o Cibercrime (Budapest Convention Against Cybercrime, editada em 23 de novembro de 2001, como marco fundamental do intercâmbio entre os países, sendo o mais importante ícone no combate ao crime cibernético na atualidade, levando em consideração a necessidade de intensificar a cooperação entre os Estados signatários e aqueles que posteriormente aderirem ao citado tratado.<sup>184</sup>

Também conhecida como Convenção de Budapeste, já conta com a adesão de mais de 65 países, dentre eles diversos países da América Latina, como Argentina (ratificou em 05/06/2018), Chile (ratificou em 20/04/2017), Costa Rica (ratificou em 22/09/2017), República Dominicana (ratificou em 07/02/2013), Panamá (ratificou em 05/03/2014), e Paraguai (ratificou em 30/07/2018). O Brasil, até a data de 14 de outubro de 2020 não havia aderido à Convenção de Budapeste.<sup>185</sup>

A Convenção de Budapeste prevê diversos critérios que devem ser seguidos pelos países signatários, tanto no âmbito do Direito Material, ao tipificar condutas, quanto no Direito Processual, estabelecendo medidas que devem ser adotadas para o sucesso das investigações. Malaquias ainda ensina que:

O mencionado acordo tem por objetivo principal a estruturação, em caráter prioritário, de uma política criminal internacional, protegendo a sociedade contra a criminalidade no *espaço cibernético* por intermédio da adoção de normas adequadas, visando a melhoria da cooperação internacional, tendo em vista que as profundas mudanças provocadas por meio da informatização, convergência e globalização permanente das redes e sistemas informatizados contribuem para aumentar o risco de que a informação digital seja utilizada para cometer inúmeros delitos, principalmente por intermédio do armazenamento e da divulgação criminosas dessas mencionadas informações, fotografias, vídeos, dados diversos, além dos conteúdos acessados e tratados ilicitamente por meio da invasão aos sistemas de redes com capilaridade regional e nacional (LAN e WAN), atingindo o vasto *backbone* internacional representado pela área de abrangência global da Internet.<sup>186</sup>

No preâmbulo da referida Convenção se observa a preocupação da comunidade europeia em intensificar a cooperação internacional entre os Estados Partes para o enfrentamento à cibercriminalidade, buscando a adoção, em caráter prioritário, de uma política criminal comum e que efetivamente proteja a sociedade

---

<sup>184</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 247.

<sup>185</sup> CONCIL OF EUROPE. **Convention on cybercrime – chart of signatures and ratifications**. Disponível em: : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>. Acesso em: 14 out. 2020.

<sup>186</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 247.

contra a criminalidade no ciberespaço, através de uma legislação adequada e que atenda os anseios da sociedade no tocante ao enfrentamento dos crimes cibernéticos.

Nos ensinamentos de Malaquias:

Prosseguindo em seu preâmbulo de intenções, a convenção pautou-se também em afirmar a necessidade de uma luta efetiva contra a cibercriminalidade, por intermédio da cooperação internacional em matéria penal, impedindo os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informatizados, de redes e dados digitais, bem como a utilização fraudulenta, assegurando a incriminação das condutas de falsidade informática, burla informática, pornografia infantil, violação de direitos autorais, definindo sanções, inclusive com tipos agravantes de comportamentos.<sup>187</sup>

As profundas mudanças provocadas pela tecnologia e pela globalização das redes informáticas gera a preocupação constante com os riscos decorrentes da utilização da *internet*, constatando-se que essas mesmas redes estão sendo utilizadas para o cometimento de crimes, e concluindo-se pela necessidade de uma política criminal comum para o enfrentamento desta problemática atual.

A Convenção se faz necessária para amenizar os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, bem como a utilização fraudulenta desses sistemas, além de amenizar os atos praticados contra as próprias pessoas, vítimas frequentes da criminalidade cibernética e que têm, além de seu patrimônio afetado, desrespeitados seus direitos fundamentais. Busca-se assegurar a efetividade das apurações criminais, resultando na incriminação dessas condutas e na responsabilização daqueles que fazem uso da tecnologia para a prática delituosa. Malaquias prossegue ensinando que:

A convenção foi profícua em delimitar competências e poderes suficientes para combater eficazmente essas infrações, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto em nível nacional como internacional, estabelecendo disposições materiais com vista a uma cooperação internacional rápida e confiável, tendo sempre presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano.<sup>188</sup>

Quanto ao direito penal material, a Convenção prevê no Título 1, da Seção 1, do Capítulo II, as infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos. O artigo 2º prevê que cada Parte adotará as medidas legislativas que se revelem necessárias para estabelecer como

---

<sup>187</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 248.

<sup>188</sup> *ibidem*

infração penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infração seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.

Neste sentido, o Código Penal brasileiro, em seu artigo 154-A, já dispõe da previsão como conduta criminosa a invasão de 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 ainda instalar vulnerabilidades neste dispositivo, para obter vantagem ilícita.

No artigo 3º da Convenção, que diz respeito à interceptação ilegítima de dados informáticos, há a previsão de que cada Parte adotará as medidas legislativas para estabelecer como infração penal, no seu direito interno, a interceptação intencional e ilegítima de dados informáticos, efetuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões eletromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infração seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

Como estudado no tópico 2.2.1.1, que trata da interceptação cibernética como meio de obtenção de prova, a Lei nº 9.296/96 traz em seu artigo 1º, parágrafo único, a previsão da interceptação do fluxo de comunicações em sistemas de informática e telemática, contemplando, portanto, esse meio de produção probatória. A mesma Lei, em seu artigo 10, prevê como conduta criminosa realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

No artigo 4º da Convenção, que trata da interferência de dados, cada Parte adotará as medidas legislativas que se revelem necessárias para estabelecer como infração penal, no seu direito interno, o ato de intencional e ilegítimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos. Esta conduta já se enquadra no artigo 154-A do CP, quanto à conduta de adulterar ou destruir dados ou informação de dispositivo alheio sem autorização.

Da mesma forma, o previsto no artigo 5º da Convenção, em relação à interferência de sistemas, em que cada Parte adotará as medidas legislativas para estabelecer como infração penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos, o mesmo artigo 154-A do CP contempla as condutas aqui elencadas no que diz respeito à instalar vulnerabilidades no sistema informático para obter vantagem ilícita.

O artigo 6º da Convenção prevê a conduta relacionada ao uso abusivo de dispositivos, em que cada Parte adotará as medidas legislativas que se revelem necessárias para estabelecer como infrações penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegítimamente, a produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infrações definidas em conformidade com os artigos 2º ao 5º da Convenção.

Além disso, no mesmo artigo há a previsão de punir-se a produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de um código de acesso ou dados informáticos semelhantes que permitam acessar um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infrações definidas nos mesmos artigos 2º ao 5º. Complementa o referido artigo 6º que a simples posse do dispositivo ou do código de acesso ilegais já configuram o crime.

O Título 2, que traz a previsão das infrações relacionadas com computadores, em seu artigo 7º trata da falsidade informática, estabelecendo que cada Parte adotará as medidas legislativas que se revelem necessárias para estabelecer como infração penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não diretamente legíveis e inteligíveis.

No artigo 8º, que trata da burla informática, cada Parte adotará as medidas legislativas que se revelem necessárias para estabelecer como infração penal, em conformidade com o seu direito interno, o ato intencional e ilegítimo, que origine a



perda de bens a terceiros através da introdução, da alteração, da eliminação ou da supressão de dados informáticos, e ainda de qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um benefício econômico ilegítimo para si ou para terceiros.

O Título 3 dispõe das infrações relacionadas com o conteúdo que é compartilhado na rede, e em seu artigo 9º trata da pornografia infantil, estabelecendo que cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infração penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima: Produzir pornografia infantil com o objetivo da sua difusão através de um sistema informático; oferecer ou disponibilizar pornografia infantil através de um sistema informático; difundir ou transmitir pornografia infantil através de um sistema informático; obter pornografia infantil através de um sistema informático para si próprio ou para terceiros; possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

No que diz respeito ao artigo 9º da Convenção, o direito penal brasileiro, através da Lei nº 8.069/90 – Estatuto da Criança e do Adolescente já contempla as condutas previstas na Convenção quanto ao enfrentamento à pornografia infantil e outras condutas relacionadas à pedofilia na *internet* em seus artigos 240, 241, 241-A, 241-B, 241-C, 241-D e 241-E.

O Título 4 da Convenção traz a previsão das infrações relacionadas com a violação do direito de autor e direitos conexos, previstas em seu artigo 10, estabelecendo que cada Parte adotará as medidas legislativas que se revelem necessárias para estabelecer como infração penal, em conformidade com o seu direito interno, a violação do direito de autor e a violação dos direitos conexos definidos pela legislação dessa Parte.

Já o Título 5 da Convenção traz a previsão de outras formas de responsabilidades e de sanções, previstas no artigo 11, estabelecendo a punição para os crimes tentados e também a punição aos coautores e partícipes.

Ainda inserido no Título 5, o artigo 12 prevê a possibilidade de punição às pessoas jurídicas, estabelecendo que cada Parte adotará medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas jurídicas possam ser consideradas responsáveis por infrações estabelecidas de acordo com a Convenção, quando cometidas em seu benefício por uma pessoa física agindo quer

individualmente ou como membro de um órgão da pessoa jurídica que exerça uma posição de direção, desde que tenha poder de representação desta pessoa jurídica; tenha autoridade para tomar decisões em nome da pessoa jurídica; ou ainda que tenha autoridade para exercer o controle da pessoa jurídica.

Há a possibilidade de a pessoa jurídica ser responsabilizada por um crime cibernético quando inexistir supervisão ou controle sobre a pessoa física, permitindo que a prática do crime tenha ocorrido.

Encerrando o Título 5 da Convenção, o artigo 13 estabelece que cada Parte adotará as medidas legislativas e outras que se revelem necessárias para assegurar que as infrações penais sejam passíveis de sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas da liberdade. Ressalta-se a importância deste artigo na Convenção, pois as sanções devem ser proporcionais ao potencial de dano de um crime cibernético para ser eficaz.

Desta forma a Convenção encerra a abordagem ao direito penal material e passa a elencar na Seção 2 os aspectos processuais penais que devem ser considerados pelos Estados Partes.

Destaca-se, dentre os procedimentos processuais, como previsto nos artigos 20 e 21, a colheita em tempo real de dados informáticos, estabelecendo que cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a recolher ou registrar, através da aplicação de meios técnicos existentes no seu território, e obrigar um fornecedor de serviços, no âmbito da sua capacidade técnica existente, a recolher ou registrar por meio da aplicação de meios técnicos no seu território, ou ainda prestar às autoridades competentes o seu apoio e assistência para recolher ou registrar, em tempo real, dados de tráfego e dados de conteúdo relativos a comunicações específicas no seu território transmitidas através de um sistema informático.

O Capítulo III da Convenção trata da cooperação internacional, que no artigo 23 estabelece que as Partes cooperarão entre si em aplicação dos instrumentos internacionais pertinentes sobre a cooperação em matéria penal, de acordos celebrados com base nas legislações uniformes ou recíprocas, e do seu direito interno, na medida mais ampla possível, para efeitos de investigações ou de procedimentos relativos à infrações penais relacionadas com sistemas e dados informáticos, ou para recolher provas sob a forma eletrônica de uma infração penal.

Quanto à cooperação internacional, nos ensinamentos de Damásio de Jesus e José Antônio Milagre:

Deste modo, a cooperação internacional ainda é um desafio para a eficácia do combate ao crime eletrônico. Os provedores, como “portas” de entrada e saída da Internet, são os primeiros a ter a possibilidade de apurar dados de usuários que sejam seus clientes. Não bastasse, no que tange o provimento de aplicações e serviços, é notório que os serviços mais utilizados no Brasil pertencem a grandes provedores de conteúdo com sede no exterior (alguns sequer com filiais físicas no Brasil). Neste contexto, em defesas envolvendo processos de quebras de sigilo de seus usuários, no Brasil, quase sempre argumentam que não estão sujeitos à jurisdição brasileira, apresentando inclusive a “lei do país sede”. Muito embora tal argumentação seja desconsiderada pelo Judiciário na grande maioria dos casos, ainda preocupa a questão do provedor no exterior que não tem filial no Brasil. Nestes casos, é importante que a cooperação internacional efetivamente se desenvolva.<sup>189</sup>

A característica da transnacionalidade nos crimes cibernéticos tem sido constantemente identificada quando uma investigação criminal está em curso, e dada a facilidade dos criminosos em encontrarem alternativas tecnológicas que burlam a identificação e colheita de provas, muitos acabam por utilizar servidores estabelecidos em território estrangeiro para a prática delituosa, o que dificulta demasiadamente a investigação e a persecução penal.

Nos ensinamentos de Jesus e Milagre quanto a necessidade de colaboração internacional:

A tecnologia da informação integrou o mundo em uma grande teia, onde todos têm acesso a tudo, pouco importando o local físico em que realmente esteja armazenado tal conteúdo. Ocorre que, para a Justiça, o local físico da prática de um ato digital tem relevância para determinar a competência judiciária.

Não incomum, os agentes buscam praticar delitos por meio de sistemas hospedados no exterior. Nestes casos, a investigação, no Brasil, necessita da cooperação de provedores (de serviço e de conexão) de fora do país, o que não é uma tarefa fácil, considerando que parte dos provedores costuma alegar que não estão sujeitos às ordens da jurisdição brasileira (isto passa a se relativizar com a aprovação do Marco Civil da Internet).<sup>190</sup>

No artigo 24 da Convenção estão estabelecidas as regras para extradição, que será admitida quando os crimes cibernéticos forem passíveis de punição na legislação dos dois Estados Partes envolvidos.

Outro aspecto bastante relevante, e que está previsto no artigo 29 da Convenção, é a possibilidade de um país solicitar a conservação das provas que se encontram em outro país. Uma Parte poderá solicitar a outra Parte que conserve os

---

<sup>189</sup> JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 180.

<sup>190</sup> *ibidem*, p. 179.

dados armazenados por meio de um sistema informático, e que se encontra no território desta outra Parte, para posterior busca e apreensão dessas provas.

Ainda em relação à obtenção de um conjunto probatório satisfatório, o artigo 34 da Convenção prevê que as Partes concederão auxílio mútuo em relação à interceptação de dados de comunicações específicas transmitidas por meio de um sistema informático.

A Convenção de Budapeste é tão abrangente no tocante ao enfrentamento dos crimes cibernéticos, que previu em seu Título 3 o que denominou de Rede 24/7, que, como descrito no artigo 35, estabelece que cada Parte disporá de um ponto de contato 24 horas por dia, 7 dias por semana, com o objetivo de assegurar a prestação de assistência imediata às investigações ou procedimentos relacionados à cibercriminalidade, o que permite o auxílio mútuo na prestação de informações técnicas, conservação de dados, além da colheita de provas.

Enfim, todos que atuam diretamente no enfrentamento ou de alguma forma colaboram para minimizar a incidência dos crimes cibernéticos entendem que este é um importante instrumento para auxiliar na persecução penal, e em se tratando de melhor adequar as investigações de crimes cibernéticos, seria um grande avanço para o Brasil poder contar com a colaboração de outros países signatários nos casos em que os crimes extrapolam os limites territoriais brasileiros.

Operadores do Direito, pesquisadores, além da comunidade acadêmica têm entendido que esta é uma importante ferramenta para o enfrentamento dos crimes cibernéticos, e neste sentido, Malaquias ensina que:

Em síntese, a mencionada convenção transformou-se em ícone no combate a cibercriminalidade, colaborando no sentido de oferecer claras diretrizes para a produção legislativa nos países signatários no sentido de seguirem o caminho da cooperação no combate ao crime cibernético, conclamando todas as nações livres a assinarem o referido pacto e envidarem esforços numa efetiva política internacional contra a cibercriminalidade.<sup>191</sup>

E ainda o mesmo autor:

Além disso, trouxe diversos preceitos relativos ao Direito Processual, delineando medidas emergenciais quanto a preservação de dados e informações relativas às investigações criminais, medidas cautelares, produção antecipada de provas, mandado de busca e apreensão, interceptação de dados para fins de investigação criminal ou instrução processual penal, medidas relativas à extradição e assistência mútua,

---

<sup>191</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 248.

intercâmbio de informações, competência jurisdicional e cooperação internacional.<sup>192</sup>

Verifica-se, portanto, que a adesão do Brasil à Convenção de Budapeste trará vários benefícios para o enfrentamento à criminalidade cibernética em nosso país. Dada as características de plurilocalidade e transnacionalidade dos cibercrimes, a cooperação dos países aderentes se mostra essencial para o melhor desempenho da aplicação da legislação penal brasileira.

---

<sup>192</sup> MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a Investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015, p. 249.

## Conclusão

A Sociedade da Informação é responsável por uma grande mudança no comportamento social mundial, e o avanço tecnológico está alterando a forma como as pessoas vivem. A disseminação e o compartilhamento de informações através do uso cada vez mais frequente da *internet* refletem diretamente nas questões sociais, políticas e econômicas de um país.

Os jovens, ainda na mais tenra idade, se interessam cada vez mais pela tecnologia inserida nos equipamentos de informática, e por outro lado, os senis, que há pouco tempo se posicionavam de forma avessa aos benefícios da tecnologia, já se rendem às facilidades que o mundo digital lhes proporcionam.

É indiscutível que as facilidades que o acesso à informação traz são extremamente úteis em todos os contextos, onde todos buscam estar atualizados e conectados com o restante do mundo. Porém, a tecnologia que tanto auxilia o cotidiano das pessoas, acaba por expô-las aos riscos das condutas daqueles que buscam o acesso à tecnologia não para fazerem parte de um mundo que busca o seu aperfeiçoamento através da informação, mas sim para a prática de crimes, os já conhecidos crimes cibernéticos.

O campo para a atuação dos criminosos é vasto, pois em razão das características do ambiente digital, não há limites territoriais ou qualquer outro tipo de barreira física, e uma simples ação criminosa pode atingir um número inestimável de pessoas, podendo abarcar inclusive diversos países, causando danos em níveis muito elevados. A ausência de barreiras físicas, que somada ao anonimato dos criminosos que é obtido através de recursos técnicos que dificultam sua identificação, e aliada à velocidade da evolução tecnológica, constituem obstáculos à persecução penal, corroborando para um dos maiores desafios da atualidade, o enfrentamento à criminalidade no ambiente digital.

A especificidades e características da criminalidade no ambiente virtual, assim como ocorre nos crimes praticados no ambiente físico, poderão variar de acordo com os aspectos sociais, culturais, econômicos, e políticos de uma nação. Há a propensão de a *internet* ser utilizada por seus usuários sem a mínima preocupação na adoção de cuidados mínimos de segurança, tornando-os vulneráveis e suscetíveis, possíveis vítimas não somente de crimes contra a honra, mas também, por exemplo, de crimes

contra o patrimônio. Não bastasse o uso da *internet* de forma indiscriminada e até irresponsável, chama-se a atenção para o fato da existência daqueles que fundamentam o seu uso no exercício da liberdade de expressão, o que não justifica extrapolar suas condutas e ferirem outros direitos de igual relevância.

Aliada à navegação por muitas vezes irresponsável de uma parcela dos usuários e o excesso do exercício do direito à liberdade de expressão, está a sensação de impunidade por parte dos cibercriminosos, os quais contam com a certeza de que jamais serão identificados e punidos, perpetuando suas atividades ilícitas e aperfeiçoando cada vez mais seu *modus operandi*. Há ainda de se mencionar o fato de que quando identificados, por uma ausência de tipificações específicas aos crimes praticados na rede, os autores, quando punidos, não recebem sanções à altura dos atos praticados.

Além das peculiaridades ligadas ao aspecto comportamental dos usuários, as próprias características dos crimes cibernéticos os tornam crimes mais difíceis de serem investigados. A plurilocalidade, a multiplicidade de vítimas, a instantaneidade e velocidade de abrangência, além da possibilidade de serem praticados de qualquer lugar do mundo, todos esse fatores somados potencializam os danos causados e não raramente desencadeiam consequências desastrosas às vítimas.

Muitos crimes cibernéticos já são processados e julgados através de leis que já vigem em nosso país, sendo a *internet* considerada apenas um meio para a prática delituosa, e poucos são as tipificações penais que mencionam as expressões “delitos informáticos”, “dispositivos informáticos”, “meio de comunicação de massa ou sistema de informática ou telemática”, “rede mundial de computadores” e “programa de computador”. O que se deixa de apreciar com a ausência de tipificações específicas é a desproporcionalidade do dano causado por um crime praticado no ambiente digital quando comparado à mesma conduta praticada no ambiente físico. Conclui-se, por certo, que a proporção do dano será infinitamente maior naquele quando comparada a este.

Os meios hoje previstos em nosso país para a apuração e processamento dos crimes cibernéticos, tanto no direito material quanto no direito processual, aparentemente não são suficientes para que a persecução penal seja efetiva, e a resposta do Estado aos criminosos acabam por tornar-se branda, quando não nula, passando a sensação de impunidade para aqueles que se aproveitam da tecnologia para a prática de crimes. Além disso, não se pode tratar os crimes comuns e aqueles

praticados na *internet* diferenciando-os apenas pelo fato de o criminoso ter usado a rede para o cometimento do delito. A extensão do dano quando o crime é praticado na *internet* é imensurável, pois a depender do grau lesivo da conduta, o restabelecimento do *status quo* da vítima torna-se inviável. Além disso, há ainda a possibilidade de milhares de usuário tornarem-se vítimas de um crime cibernético através de um simples apertar de uma tecla.

Dessa maneira, quando a *internet* é utilizada para a prática de crimes, deveria o criminoso sofrer uma sanção à altura do potencial do dano que causou ou poderia ter causado, e haveria, portanto, a distinção na apuração entre os crimes praticados no ambiente físico e aqueles praticados no ambiente digital, onde somente uma tipificação adequada e sancionada à altura do potencial do dano poderia então atender aos anseios da sociedade.

Durante o transcorrer do presente trabalho, alguns aspectos relacionados aos crimes cibernéticos restaram demonstrados como entraves no seu enfrentamento, gerando uma reflexão sobre a possibilidade das melhorias que ainda poderão ser buscadas na persecução penal e sua efetividade.

Uma das questões mais desafiadoras quanto a persecução penal dos crimes cibernéticos é a correta determinação da jurisdição e da competência, isso em virtude dessas espécies de crimes possuírem a peculiar característica da plurilocalidade, podendo atingir ainda a transnacionalidade, características estas que os diferem dos demais crimes praticados no ambiente físico, o que demanda atenção especial na correta aplicação da lei processual penal. Por se tratar de delitos que, ao ocuparem o espaço virtual, desencadeiam diversos resultados, em diversos locais diferentes, além de atingirem múltiplas vítimas, a determinação jurisdicional para os crimes cibernéticos tem se mostrado uma tarefa bastante complexa e que ainda é bastante divergente.

Não bastasse a plurilocalidade e transnacionalidade dos crimes cibernéticos, a multiplicidade de agentes ativos, bem como o número imensurável de vítimas que podem ser afetadas por uma única conduta, a busca pela apuração e colheita de um conjunto probatório satisfatório é, sem dúvida, um dos grandes obstáculos enfrentados pelos agentes públicos no enfrentamento à cibercriminalidade. A obtenção da prova no ambiente digital é tarefa extremamente complexa, e em virtude das características dos crimes cibernéticos, faz com que a investigação criminal nesta



área seja tarefa onde o conhecimento técnico específico e altamente qualificado seja fundamental para o êxito das investigações.

A migração da criminalidade do ambiente físico para o ambiente virtual criou um fator extra de complexidade na apuração de um crime cibernético, onde as provas, que antes deixavam vestígios palpáveis, hoje precisam ser buscadas distante dos olhos de quem investiga. Os crimes cibernéticos, quando comparados aos crimes que deixam vestígios físicos, encontram problemática voltada a não dispersão das evidências, e que por se encontrarem em ambiente digital, tornam-se mais suscetíveis ao perecimento. Referida circunstância demanda um cuidado especial na sua abordagem, e que, diferentemente dos crimes praticados fora do ambiente digital, por mais desafiador que ainda seja coletar provas no ambiente físico, e por mais que a correta preservação do local do crime ainda seja um desafio, as evidências permanecem fisicamente presentes.

Diante dos desafios enfrentados na busca de um conjunto probatório robusto e satisfatório é fundamental que o Estado disponibilize aos agentes públicos treinamento técnico constante para acompanhar a evolução tecnológica para que tenham exato entendimento de como os criminosos atuam e quais os meios empregados por eles para a prática delituosa. Além disso, os meios de obtenção de provas hoje previstos no ordenamento jurídico penal devem ser adequados aos desafios encontrados no ambiente digital.

As atividades de investigação policial que envolvem os crimes cibernéticos se depararam com inúmeros desafios diante do aperfeiçoamento da tecnologia e do surgimento de novos meios de execução das condutas ilícitas que são adotados pelos criminosos. Na tentativa constante de se esquivar da persecução penal, o cibercriminoso busca alternativas que impedem sua identificação e, por consequência, sua responsabilização pelos crimes que pratica. Dentre os meios utilizados para esta finalidade, a navegação na *Dark Web* tem sido a preferida, onde o objetivo é a obtenção do anonimato absoluto, tornando-se quase que impossível a identificação do usuário.

A identificação de criminosos nesta área da *internet* se mostra extremamente complexa e desafiadora, pois além do conteúdo ilícito ser criptografado, há ainda a problemática da utilização de diversos servidores diferentes para a comunicação, podendo estes, quando e se identificados, estarem localizados em diversos países, gerando então os conflitos de jurisdição anteriormente estudados.

Com o objetivo de minimizar os danos causados pelos crimes praticados no ambiente virtual, deverá o Estado adotar instrumentos aditivos para o enfrentamento desta modalidade criminosa. Um desses instrumentos é a introdução da educação digital e a adoção de políticas públicas voltadas à conscientização dos cidadãos e cidadãs, visando aprimorar os conhecimentos no uso da tecnologia. Seria imprudente deixar de admitir que se faz necessário um conjunto de ações educacionais que permita a todos alcançar um nível de saber minimamente necessário sobre os aspectos positivos e negativos relacionados à era digital.

A educação tem um papel fundamental na formação das pessoas desde a mais tenra idade. Oportunizar à criança o acesso à educação digital permite estimular seus conhecimentos para obter um melhor convívio social, estabelecer o respeito ao próximo como sendo a regra, gerar responsabilidades e fundamentalmente exercer a cidadania tornar-se um bom cidadão conectado.

Consiste em grande desafio ensinar como as pessoas devem fazer uso da tecnologia inserida nesses aparelhos, com bom senso e ética, de modo que minimize os danos ocasionados por ações pelo mau uso e práticas criminosas na rede. É de suma importância que o Estado estabeleça conteúdos educacionais voltados para a capacitação do uso da tecnologia planos de conscientização com o objetivo de demonstrar a todos a necessidade de ter-se um nível de discernimento suficiente para assimilar as informações disponíveis na *internet* e tirar o melhor proveito da conectividade para o desenvolvimento de suas capacidades.

Outro instrumento aditivo para o enfrentamento da cibercriminalidade cibernética, e não menos importante, trata da reavaliação e adequação legislativa do ordenamento jurídico penal brasileiro no sentido de melhor adequar as condutas ilícitas praticadas na *internet* aos tipos penais já existentes, além da criminalização de condutas ainda não previstas, o que demonstra a importância do estabelecimento de uma legislação robusta e eficiente com o objetivo de contribuir para a obtenção de melhores resultados nas investigações nos crimes cibernéticos e na sua persecução penal. O Estado tem o dever de ser mais efetivo ao prestar sua tutela, e tanto o Código Penal quanto o Código de Processo Penal deverão passar por alterações visando maior efetividade das leis.

Diante da evolução tecnológica e do aprimoramento dos mecanismos utilizados pelos criminosos para a prática delitiva no ambiente cibernético, observa-se uma lacuna legislativa, e que acaba por permitir a maior incidência dos crimes

cibernéticos. Há de se avaliar uma alternativa no sentido de as casas legislativas dedicarem maiores esforços para adequar a legislação à nova realidade da sociedade, o que já vem ocorrendo em diferentes países.

Um conjunto de normas jurídicas bem estruturadas será instrumento fundamental para o enfrentamento dos crimes cibernéticos, e as mudanças de âmbito legislativo e nas atividades jurisdicionais são imprescindíveis, permitindo que o Estado preste sua tutela de forma mais efetiva, não somente contribuindo para a evolução do Direito, mas proporcionando melhores condições para aplicação da lei.

O último instrumento estudado sobre os aditivos ao enfrentamento dos crimes cibernéticos diz respeito à Convenção de Budapeste, que visa tipificar diversas condutas ilícitas praticadas na *internet*, além de estabelecer procedimentos processuais comuns entre os países signatários, possibilitando ainda a cooperação internacional para o sucesso das investigações dos crimes que tenham como uma de suas características a transnacionalidade.

Com a adesão à referida Convenção busca-se assegurar a efetividade das apurações criminais, resultando na incriminação dessas condutas e na responsabilização daqueles que fazem uso da tecnologia para a prática delituosa. O Brasil ainda não aderiu à Convenção, e todos que atuam diretamente no enfrentamento ou de alguma forma colaboram para minimizar a incidência dos crimes cibernéticos entendem que este é um importante instrumento para auxiliar na persecução penal, e em se tratando de melhor adequar as investigações dos crimes cibernéticos, seria um grande avanço para o Brasil poder contar com a colaboração de outros países signatários nos casos em que os crimes extrapolam os limites territoriais brasileiros.

Conclui-se, portanto, que o enfrentamento à criminalidade cibernética tornou-se um dos maiores desafios da atualidade, e que ainda há um longo caminho a ser percorrido na busca por um conjunto de leis capaz de atender à altura as demandas provenientes da criminalidade no ambiente digital.

Além disso, na tentativa de minimizar seus efeitos, fica evidenciado que o Estado deve realizar investimentos em políticas públicas voltadas à educação digital e campanhas de conscientização para o uso adequado e seguro da *internet*. Investimentos para a capacitação adequada dos agentes públicos, aquisição de equipamentos de última geração e tecnologia de ponta também devem ser levados em consideração.

A somatória de todas essas ações irá contribuir substancialmente para que os criminosos deixem de se sentir tão confortáveis no ambiente digital e passem a ser identificados e punidos. Deverá o Estado, portanto, prestar sua tutela de maneira mais efetiva no sentido de enfrentar esta modalidade criminosa e que aflige todo o mundo contemporâneo, identificando seus autores, punindo-os e por consequência minimizando os danos causados à sociedade.

## Referências

- ALMEIDA, Patrícia Martinez; SILVEIRA, Vladmir Oliveira. O direito ao esquecimento e a privacidade. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 619-643.
- BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do marco civil da internet**. Rio de Janeiro: Brasport, 2016, p. 28.
- BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELI, Guilherme. **Investigação digital em fontes abertas**. 2. ed. Rio de Janeiro: Brasport, 2017.
- BARRETO JUNIOR, Irineu Francisco. Proteção de dados pessoais na *internet*: o marco civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 405-430.
- BAUMAN, Zygmunt. **Globalização: as consequências humanas**. Rio de Janeiro: Jorge Zahar, 1999.
- BAUMAN, Zygmunt; DAVID, Lyon; tradução Carlos Alberto Medeiros. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013.
- CAMILLO, Carlos Eduardo Nicoletti. O fenômeno do fakenews e a sua repercussão na responsabilidade civil no sistema jurídico brasileiro. *In*: RAIS, Diogo (Org.). **Fakenews – a conexão entre a desinformação e o direito**. São Paulo: Revista dos Tribunais, 2018, p. 221-233.
- CASTELLS, Manuel; tradução Joana Angélica d’Avila Melo. **Ruptura: a crise da democracia liberal**. Rio de Janeiro: Zahar, 2018.
- DOMINGOS, Fernanda Teixeira Souza. A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual infantil *online*. *In*: SILVA, Ângelo Roberto Ilha da (org.). **Crimes cibernéticos**. 2. ed. Porto Alegre: Livraria do advogado, 2018, p. 235-253.
- FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2. ed. São Paulo: Saraiva, 2016.
- FREIRE, Paulo. **Pedagogia da autonomia: saberes necessários à prática educativa**. 63. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2020.
- FULLER, Greice Patrícia. O Direito criminal difuso, a dignidade da pessoa humana e a mídia na sociedade da informação. **VII Congresso brasileiro da sociedade da informação regulação da mídia na sociedade da informação**, 2014, p. 131-141.

FULLER, Greice Patrícia; BARRETO JUNIOR, Irineu Francisco. Desinformação e covid-19 no Brasil: desafios e limites do enquadramento penal da disseminação de notícias falsas. In: LIMA, Fernando Rister de Souza; MARTINI, Sandra Regina; SMANIO, Gianpaolo Poggio; WALDMAN, Ricardo Libel (coords.). **Covid-19 e os impactos no direito: mercado, Estado, trabalho, família, contratos e cidadania**. São Paulo: Almedina, 2020, p. 39-52.

GROSS, Clarissa Piterman. *Fakenews* e democracia: discutindo o *status* normativo do falso e a liberdade de expressão. In: RAIS, Diogo (Org.). **Fakenews – a conexão entre a desinformação e o direito**. São Paulo: Revista dos Tribunais, 2018, p. 153-174.

GUIDI, Guilherme Berti de Campos; REZEK Francisco. Crimes na *internet* e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 277-288.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

JONAS, Hans; tradução do original alemão Luiz Barros Montez, Marijane Lisboa. **O princípio responsabilidade: Ensaio de uma ética para a civilização tecnológica**. Rio de Janeiro: PUC – Rio, 2006.

KIST, Dario José. **Prova digital no processo penal**. Leme/SP: JH Mizuno, 2019.

KRETSCHMANN, Ângela; WENDT, Emerson. **Tecnologia da informação & direito**. Porto Alegre: Livraria do advogado, 2018.

KUIAVA, Evaldo Antonio. A responsabilidade como princípio ético em H. Jonas e E. Levinas: Uma aproximação. **Veritas**, v.51, n.2, Porto Alegre, 2006, pp. 55-60.

MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova – a investigação criminal em busca da verdade**. 2. ed. Curitiba: Juruá, 2015.

MARCACINI, Augusto Tavares Rosa. Provas digitais: limites constitucionais e o marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei nº 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 455-473.

MEYER-PFLUG, Samantha Ribeiro; LEITE, Flavia Piva Almeida. A liberdade de expressão e o direito à privacidade no marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coords.). **Direito & Internet III – Tomo I: marco civil da internet (Lei n. 12.965/2104)**. São Paulo: Quartier Latin, 2015, p. 435.

RAIS, Diogo (org.). **Fakenews – a conexão entre a desinformação e o direito**. São Paulo: Revista dos Tribunais, 2018.

SCHREIBER, Anderson. Marco civil da *internet*: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro. In: DE

LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 277-305.

SOUZA, Carlos Affonso Pereira de. As cinco faces da proteção à liberdade de expressão no marco civil da *internet*. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira (coords.). **Direito & Internet III – Tomo II: marco civil da internet (Lei n. 12.965/2014)**. São Paulo: Quartier Latin, 2015, p. 377-408.

TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil: livro verde**. Brasília: Ministério da Ciência e Tecnologia, 2000.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 7. ed. Bahia: Podvim, 2012.

WOLFF, Rafael. Infiltração de agentes por meio virtual. In: SILVA, Ângelo Roberto Ilha da (org.). **Crimes cibernéticos**. 2. ed. Porto Alegre: Livraria do advogado, 2018, p. 217-234.

## Documentos Eletrônicos

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 02 jul. 2019.

BRASIL. **Código Penal Brasileiro. Decreto - Lei nº 2.848, de 7 de dezembro de 1940**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/Del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm). Acesso em: 03 jul. 2019.

BRASIL. **Código de Processo Penal. Decreto - Lei nº 3.689, de 3 de outubro de 1941**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/Del3689Compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm). Acesso em: 04 jul. 2019.

BRASIL. **Lei nº 4.737, de 15 de julho de 1965**. Institui o Código Eleitoral. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l4737.htm](http://www.planalto.gov.br/ccivil_03/leis/l4737.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 7.170, de 14 de dezembro de 1983**. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l7170.htm](http://www.planalto.gov.br/ccivil_03/leis/l7170.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l7716.htm](http://www.planalto.gov.br/ccivil_03/leis/l7716.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o estatuto da criança e do adolescente e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8069.htm](http://www.planalto.gov.br/ccivil_03/leis/l8069.htm). Acesso em: 02 jul. 2019.

BRASIL. **Lei nº 8.137, de 27 de dezembro de 1990.** Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L8137.htm](http://www.planalto.gov.br/ccivil_03/leis/L8137.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/I9099.htm](http://www.planalto.gov.br/ccivil_03/leis/I9099.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 9.279, de 14 de maio de 1996.** Regula direitos e obrigações relativos à propriedade industrial. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/I9279.htm](http://www.planalto.gov.br/ccivil_03/leis/I9279.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/I9296.htm](http://www.planalto.gov.br/ccivil_03/leis/I9296.htm). Acesso em: 02 jul. 2019.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998.** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/I9609.htm](http://www.planalto.gov.br/ccivil_03/leis/I9609.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 10.826, de 22 de dezembro de 2003.** Dispõe sobre registro, posse e comercialização de armas de fogo e munição, sobre o Sistema Nacional de Armas – Sinarm, define crimes e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/LEIS/2003/L10.826.htm](http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.826.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 11.343, de 23 de agosto de 2006.** Institui o sistema nacional de políticas públicas sobre drogas – Sisnad; prescreve medida para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para a repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2006/lei/l11343.htm](http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm). Acesso em: 03 jul. 2019.

BRASIL. **Lei nº 11.829, de 25 de novembro de 2008.** Altera a lei nº 8.069, de 13 de julho de 1990 – Estatuto da criança e do adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na *internet*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2007-2010/2008/Lei/L11829.htm#art1](http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm#art1). Acesso em: 03 jul. 2019.

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. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acesso em: 31 jul. 2019.



BRASIL. **Lei nº 12.850, de 02 de agosto de 2013.** Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção de prova, infrações penais correlatas e o procedimento criminal; altera o decreto-lei nº 2.848, de 7 de dezembro de 1940 (código penal); revoga a lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/lei/l12850.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm). Acesso em: 03 jul. 2019.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 04 jul. 2019.

BRASIL. **Lei nº 13.441, de 8 de maio de 2017.** Altera a Lei 8.609, de 13 de julho de 1990 (estatuto da criança e do adolescente), para prever a infiltração de agentes de polícia na *internet* com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2017/Lei/L13441.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm). Acesso em: 02 jul. 2019.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13718.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm). Acesso em: 31 jul. 2019.

BRASIL. **Lei nº 13.964 de 24 de dezembro de 2019.** Aperfeiçoa a legislação penal e processual penal. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2019/Lei/L13964.htm#art3](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm#art3). Acesso em: 08 out. 2020.

BRASIL. Ministério Público Federal. **Nota técnica do grupo de apoio sobre criminalidade cibernética sobre a convenção do cibercrimes. (Convenção de Budapeste). 2018.** Disponível em: [http://www.mpf.mp.br/pgr/documentos/2CCR\\_NotaTecnica\\_ConvencaoBudapeste.pdf](http://www.mpf.mp.br/pgr/documentos/2CCR_NotaTecnica_ConvencaoBudapeste.pdf). Acesso em: 26 mar. 2019.

BRASIL. Superior Tribunal de Justiça. **RSE – 07010282020168020082 AL 0701028-20.2016.8.02.0082.** Disponível em: <https://tj-al.jusbrasil.com.br/jurisprudencia/689268082/recursoem-sentido-estrito-rse7010282020168020082-al-0701028-2020168020082/inteiro-teor-689268091>. Acesso em: 06 abr. 2019.

BRASIL. Superior Tribunal de Justiça. **Conflito de competência nº 97.372 – SP.** Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/19134047/conflito-de-competencia-cc-97372-sp-2008-0147300-8/inteiro-teor-19134048?ref=juris-tabs>. Acesso em: 07 out. 2019.

BRASIL. Superior Tribunal de Justiça. **Conflito de competência nº 145.576 – MA.** Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/339952309/conflito-de-competencia-cc-145576-ma-2016-0055604-1/inteiro-teor-339952319>. Acesso em: 07 out. 2019.

BRASIL. Superior Tribunal de Justiça. **Conflito de competência nº 156.284 – PR.** Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/552870809/conflito-de-competencia-cc-156284-pr-2018-0008775-5/inteiro-teor-552870818?ref=juris-tabs>. Acesso em: 07 out. 2019.

BRASIL. Supremo Tribunal Federal. **STF conclui julgamento e restringe prerrogativa de função a parlamentares federais.** Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=377332>. Acesso em: 21 mar. 2019.

BRASIL. Superior Tribunal Federal. **Súmula 145.** Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=2119>. Acesso em: 05 out. 2020.

CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019.

CONCIL OF EUROPE. **Convention on cybercrime – chart of signatures and ratifications.** Disponível em: : <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>. Acesso em: 14 out. 2020.

CONVENÇÃO SOBRE O CIBERCRIME. **Convenção de Budapeste. 2001.** Disponível em [http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf). Acesso em: 14 out. 2020.

ESPAÑA. **Código Penal Español.** Disponível em: [https://oig.cepal.org/sites/default/files/2003\\_esp\\_codpenal-actualizado2011.pdf](https://oig.cepal.org/sites/default/files/2003_esp_codpenal-actualizado2011.pdf). Acesso em: 04 nov. 2020.

FGV. **31ª Pesquisa Anual de Administração e Uso de Tecnologia da Informação nas Empresas/2020.** Disponível em: [https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados\\_0.pdf](https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados_0.pdf). Acesso em: 08 out. 2020.

FOLHA DE SÃO PAULO / UOL. **Veja o passo a passo da notícia falsa que acabou em tragédia no Guarujá.** Disponível em: <https://www1.folha.uol.com.br/cotidiano/2018/09/veja-o-passo-a-passo-da-noticia-falsa-que-acabou-em-tragedia-em-guaruja.shtml>. Acesso em: 05 ago. 2019.

GRIGORI, Pedro. **Pública: agência de jornalismo investigativo.** 20 projetos de lei no Congresso pretendem criminalizar fake news. Disponível em:

<https://apublica.org/2018/05/20-projetos-de-lei-no-congresso-pretendem-criminalizar-fake-news/> . Acesso em: 05 ago. 2019.

GUIDI, Guilherme Berti de Campos; REZEK Francisco. Crimes na *internet* e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista Brasileira de Políticas Públicas**. Brasília, v. 8, nº 1, 2018, p. 276-288. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/5244/pdf>. Acesso em: 16 jul. 2019.

IBGE. **PNAD 2018 - Pesquisa Nacional por Amostra de Domicílio**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/27515-pnad-continua-tic-2018-internet-chega-a-79-1-dos-domicilios-do-pais>. Acesso em: 08 out. 2020.

LISBOA, Roberto Senise. **Direito na sociedade da informação**. São Paulo: Revista dos Tribunais, 2006. Disponível em: [https://scholar.google.com.br/citations?user=85XbR84AAAAJ&hl=pt-BR#d=gs\\_md\\_cita-d&u=%2Fcitations%3Fview\\_op%3Dview\\_citation%26hl%3Dpt-BR%26user%3D85XbR84AAAAJ%26citation\\_for\\_view%3D85XbR84AAAAJ%3AzYL M7Y9cAGgC%26tzom%3D180](https://scholar.google.com.br/citations?user=85XbR84AAAAJ&hl=pt-BR#d=gs_md_cita-d&u=%2Fcitations%3Fview_op%3Dview_citation%26hl%3Dpt-BR%26user%3D85XbR84AAAAJ%26citation_for_view%3D85XbR84AAAAJ%3AzYL M7Y9cAGgC%26tzom%3D180). Acesso em: 08 out. 2020.

NORTON. **Norton cyber security insights report global results 2018**. Disponível em: [https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018\\_Norton\\_LifeLock\\_Cyber\\_Safety\\_Insights\\_Report\\_US\\_Media\\_Deck.pdf?promocode=DEFAULTWEB%20](https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_US_Media_Deck.pdf?promocode=DEFAULTWEB%20). Acesso em: 08 out. 2020.

ONU. **UNCTAD 2017 – United nations conference on trade and development**. Disponível em: [https://unctad.org/en/PublicationsLibrary/wir2017\\_en.pdf](https://unctad.org/en/PublicationsLibrary/wir2017_en.pdf). Acesso em 25 jul. 2019.

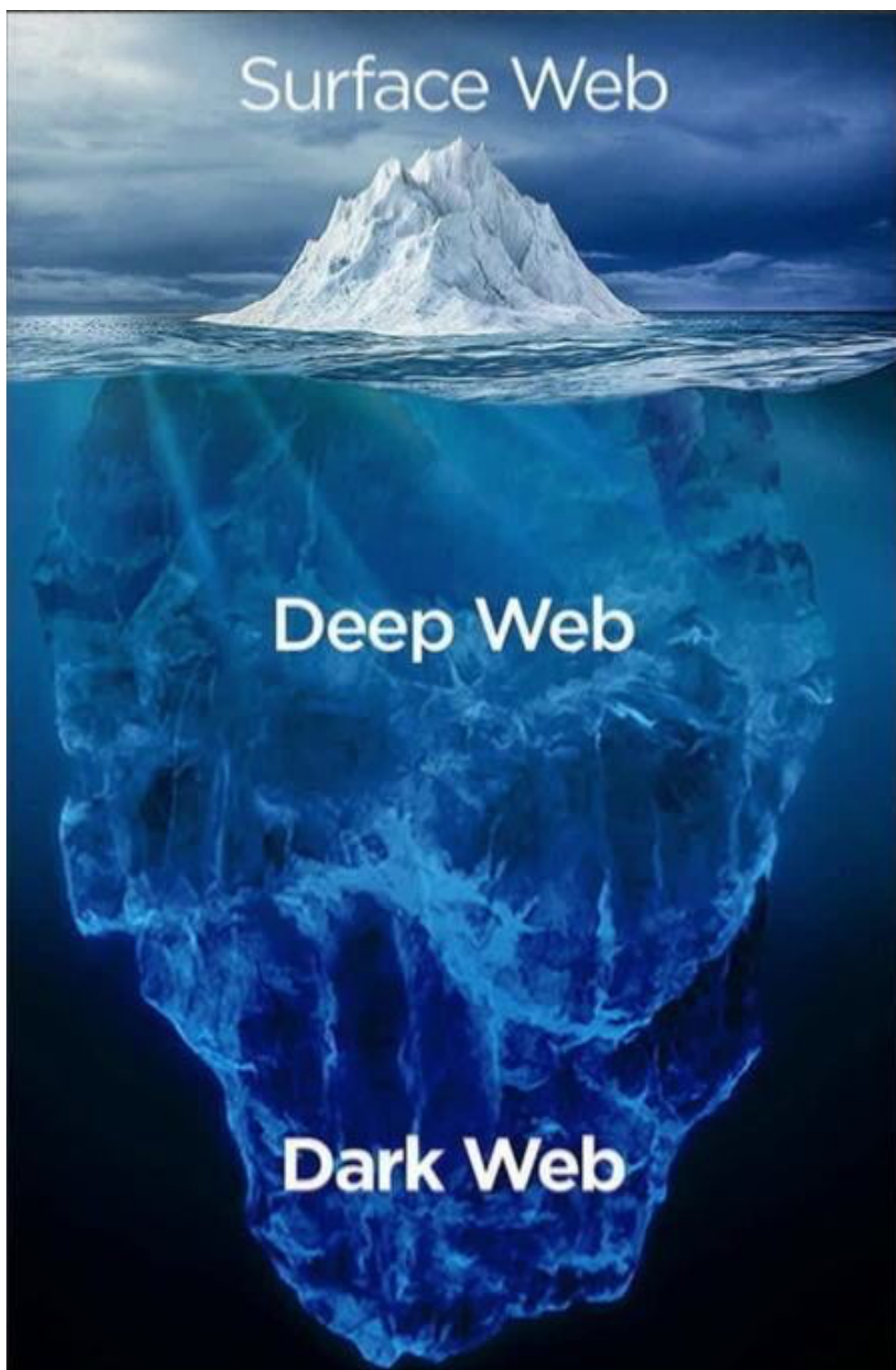
PORTUGAL. **Lei nº 109 de 15 de setembro de 2009**. Lei do Cibercrime. Disponível em: [http://www.pgdlisboa.pt/leis/lei\\_mostra\\_articulado.php?nid=1137&tabela=leis&fica=1&pagina=1&so\\_miolo=S](http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis&fica=1&pagina=1&so_miolo=S). Acesso em: 04 nov. 2020.

PROJETO TOR. **História**. Disponível em: <https://www.torproject.org/pt-BR/>. Acesso em: 19 jul. 2019.

SYDOW, Spenser Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/pt-br.php>. Acesso em: 26 mar. 2019.

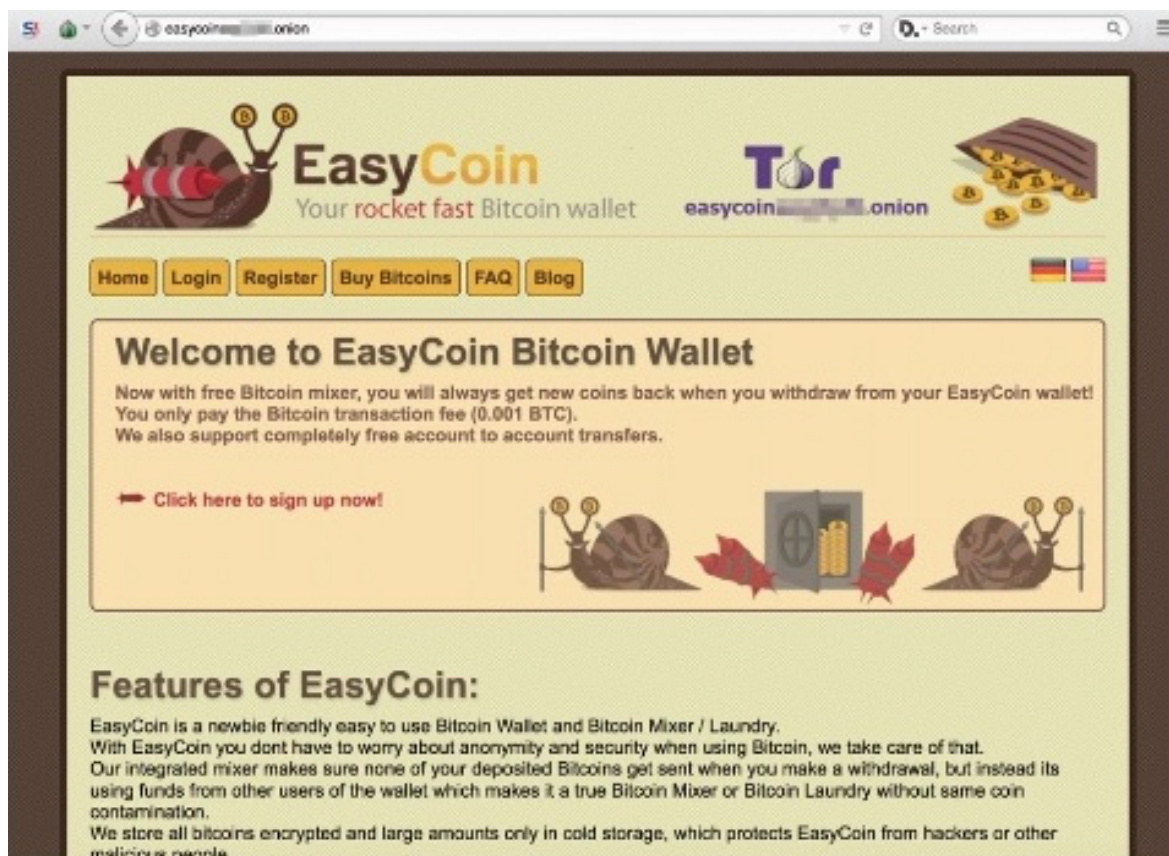
## Anexo A – Imagens ilustrativas da navegação na *Dark Web*

Imagem 01



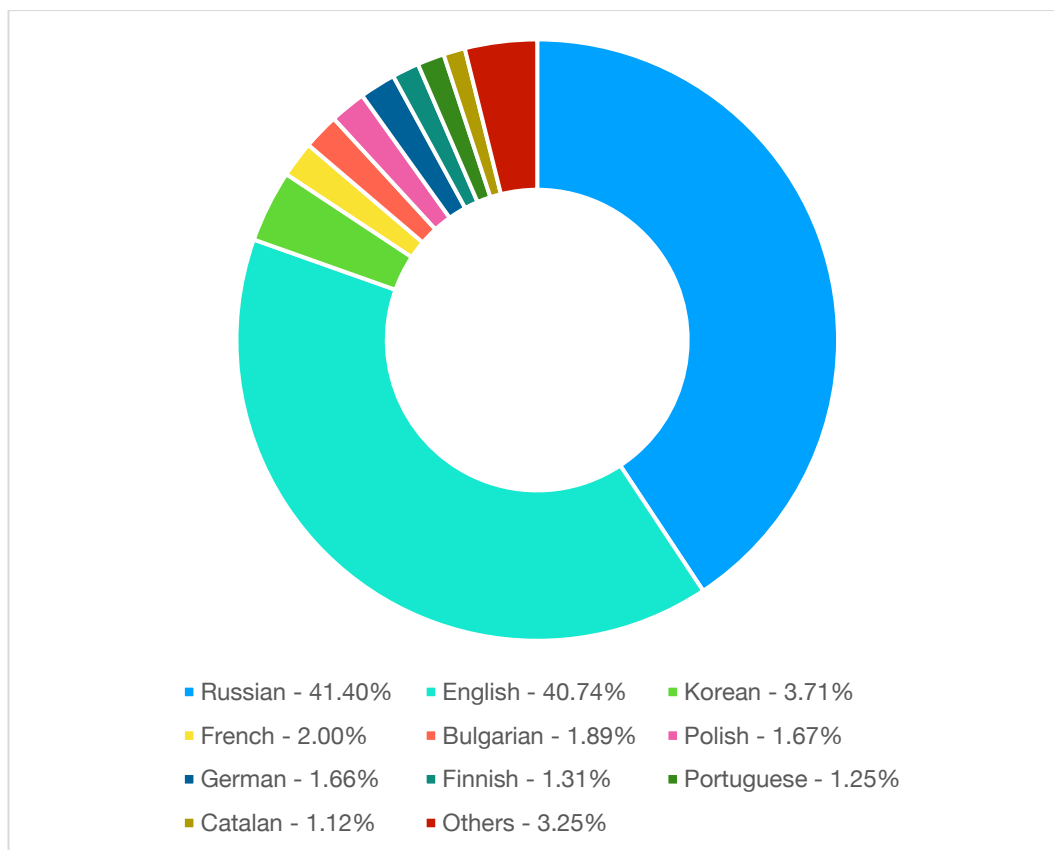
Clássica imagem do *iceberg*, que ilustra com muita propriedade as camadas de acesso à *internet*.

Imagem 02

Serviço de lavagem de Bitcoin EasyCoin <sup>193</sup>

<sup>193</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 22. Texto original: *EasyCoin Bitcoin-laundering service.*

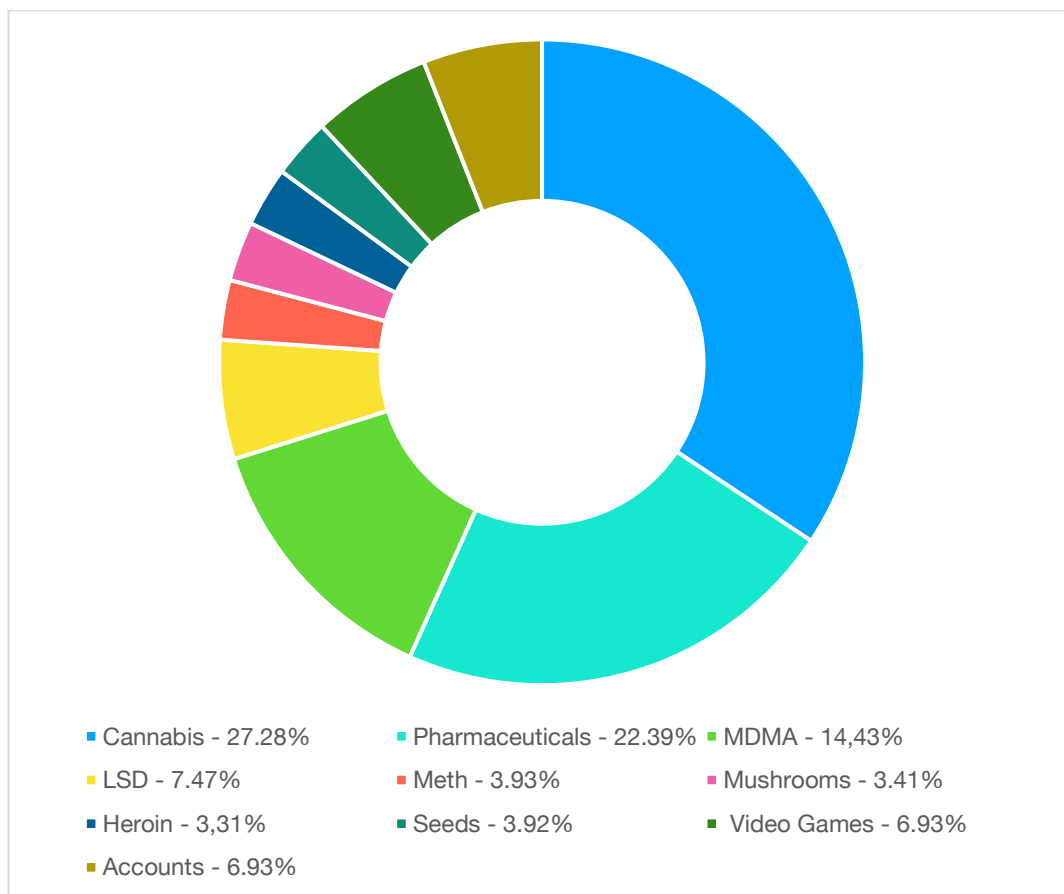
Imagem 03



Os idiomas mais populares com base no número de URLs com conteúdo <sup>194</sup>

<sup>194</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 10. Texto original: *Most popular languages based on the number of URLs with content using them.*

Imagem 04



Detalhamento do comprador com base em dados obtidos em 3 de junho de 2015<sup>195</sup>

<sup>195</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p.11. Texto original: *Buyer breakdown based on data pulled on 3 June 2015.*



Imagem 05

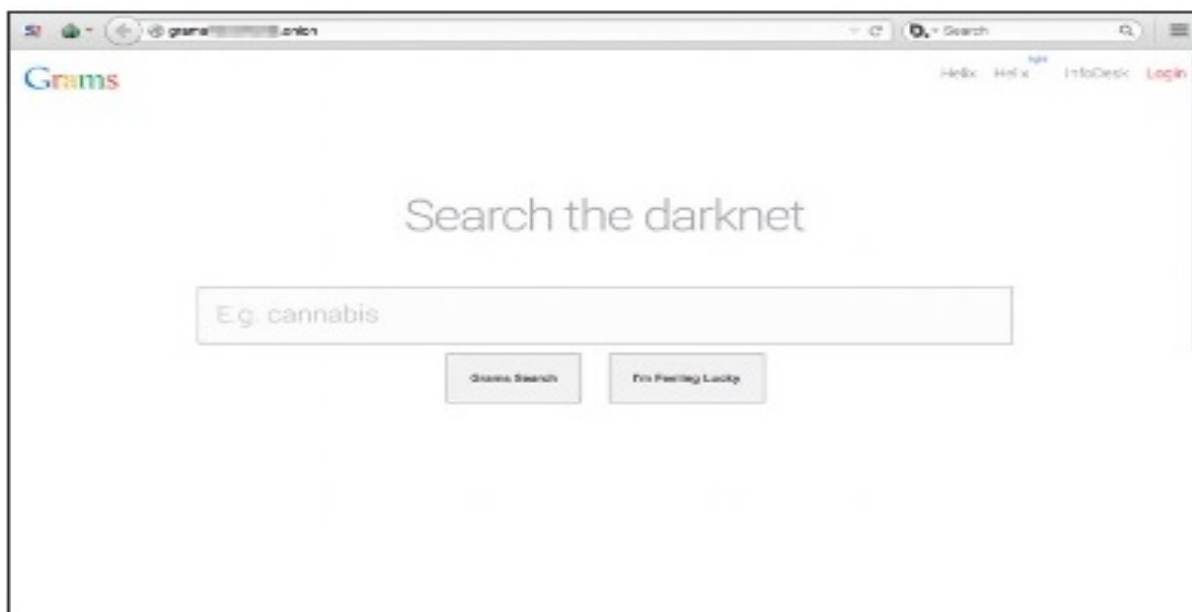


A disponibilidade de narcóticos ilegais varia muito na Deep Web. Alguns sites vendem de tudo, desde produtos relativamente inofensivos (tabaco contrabandeado) até cannabis, psicodélicos, cocaína e outros.<sup>196</sup>

<sup>196</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p.20. Texto original: *The availability of illegal narcotics varies a lot on the Deep Web. Some sites sell everything from the relatively tame (contraband tobacco) to cannabis, psychedelics, cocaine, and others.*



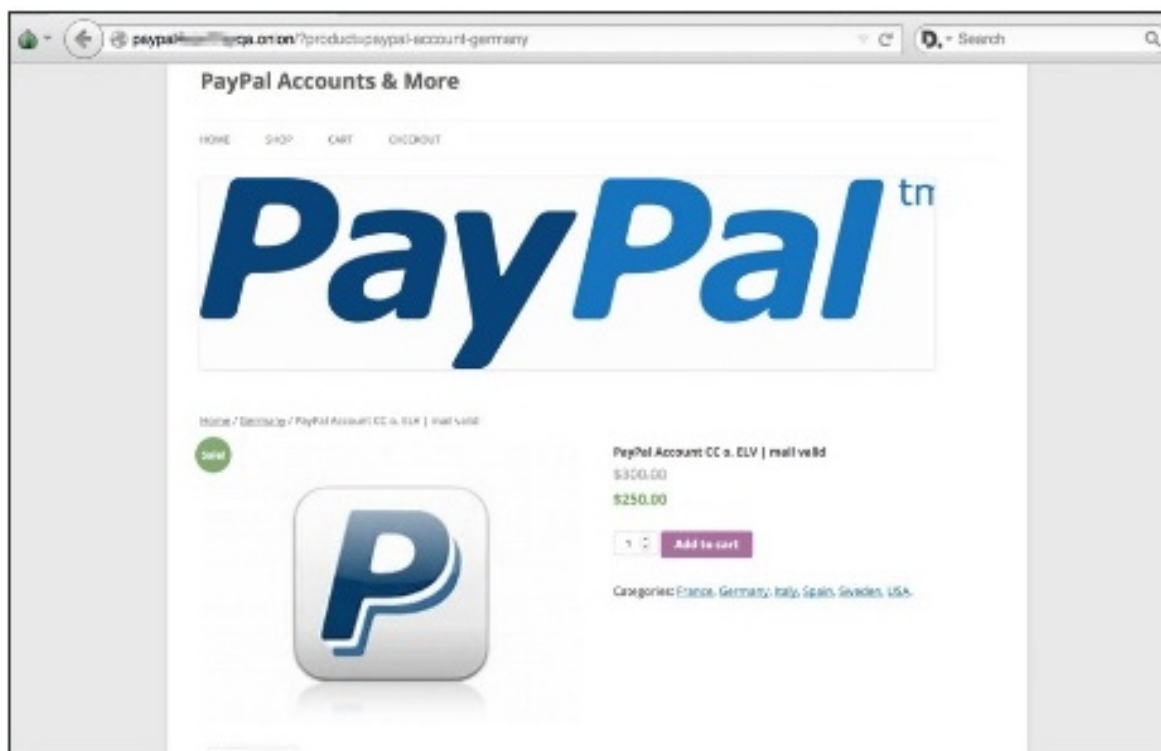
Imagem 06

Grams - o motor de busca Deep Web para drogas. <sup>197</sup>

---

<sup>197</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p.20. Texto original: *Grams – the Deep Web search engine for drugs.*

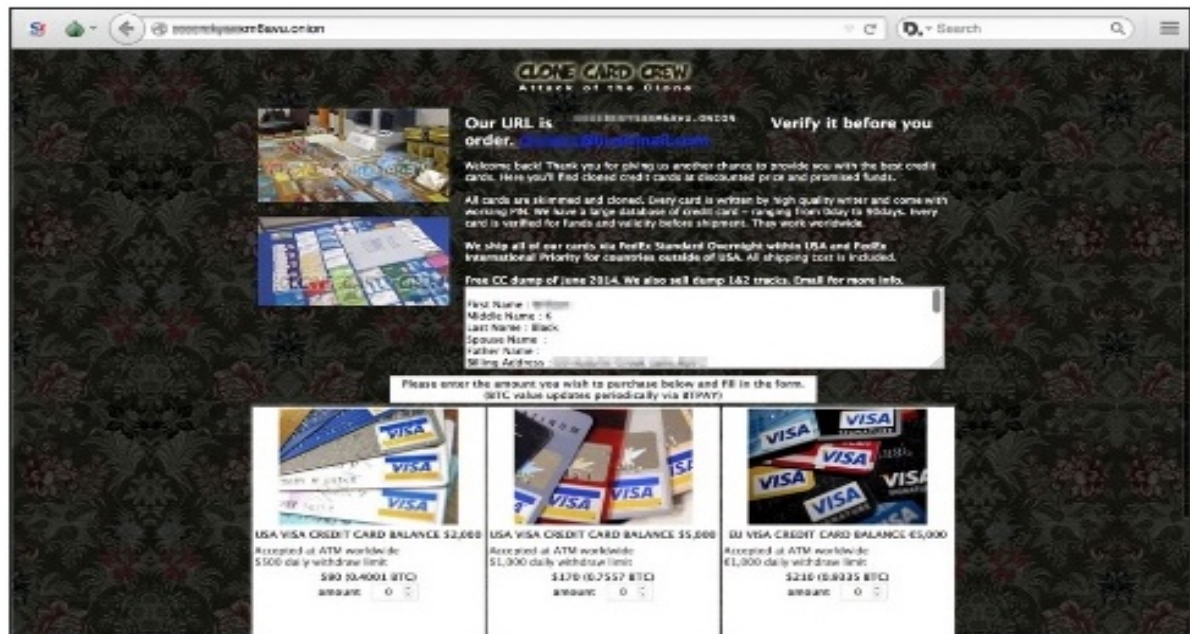
Imagem 07



Contas do PayPal alemãs verificadas roubadas (saldo de US \$ 500-700) à venda por US \$ 250<sup>198</sup>

<sup>198</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 25. Texto original: Stolen verified German PayPal accounts (US\$500-700 balance) for sale for US\$250.

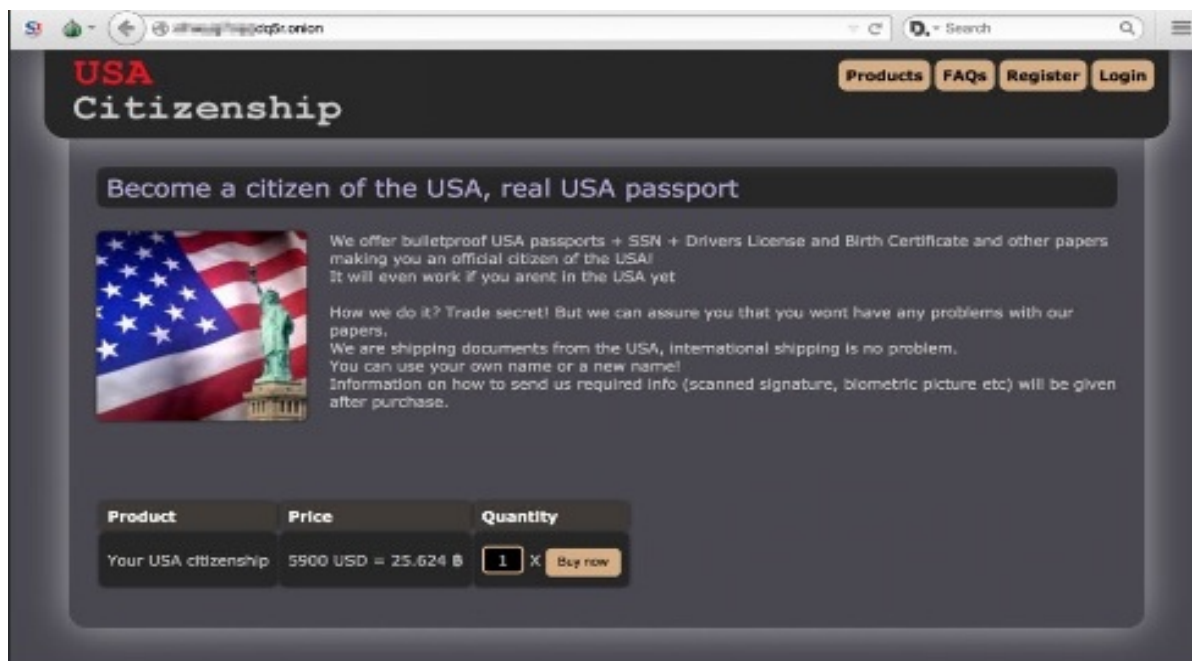
Imagem 08



Réplica de cartões de crédito criados com dados roubados. 199

<sup>199</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 26. Text0 original: Replica credit cards created with stolen details.

Imagem 09



The screenshot shows a web browser window with the URL [www.uscitizenship.com](http://www.uscitizenship.com). The page features a dark header with the text "USA Citizenship" and navigation buttons for "Products", "FAQs", "Register", and "Login". Below the header, a main heading reads "Become a citizen of the USA, real USA passport". To the left of the text is an image of the American flag and the Statue of Liberty. The text describes the offer: "We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA! It will even work if you arent in the USA yet". It also includes a disclaimer: "How we do it? Trade secret! But we can assure you that you wont have any problems with our papers. We are shipping documents from the USA, international shipping is no problem. You can use your own name or a new name! Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase." At the bottom, there is a table with columns for "Product", "Price", and "Quantity".

Product	Price	Quantity
Your USA citizenship	5900 USD = 25.624 B	1 X Buy now

Cidadania americana à venda por US\$ 6.000.<sup>200</sup>

<sup>200</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web**. Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 27. Texto original: U.S. citizenship for sale for at least US\$6,000.

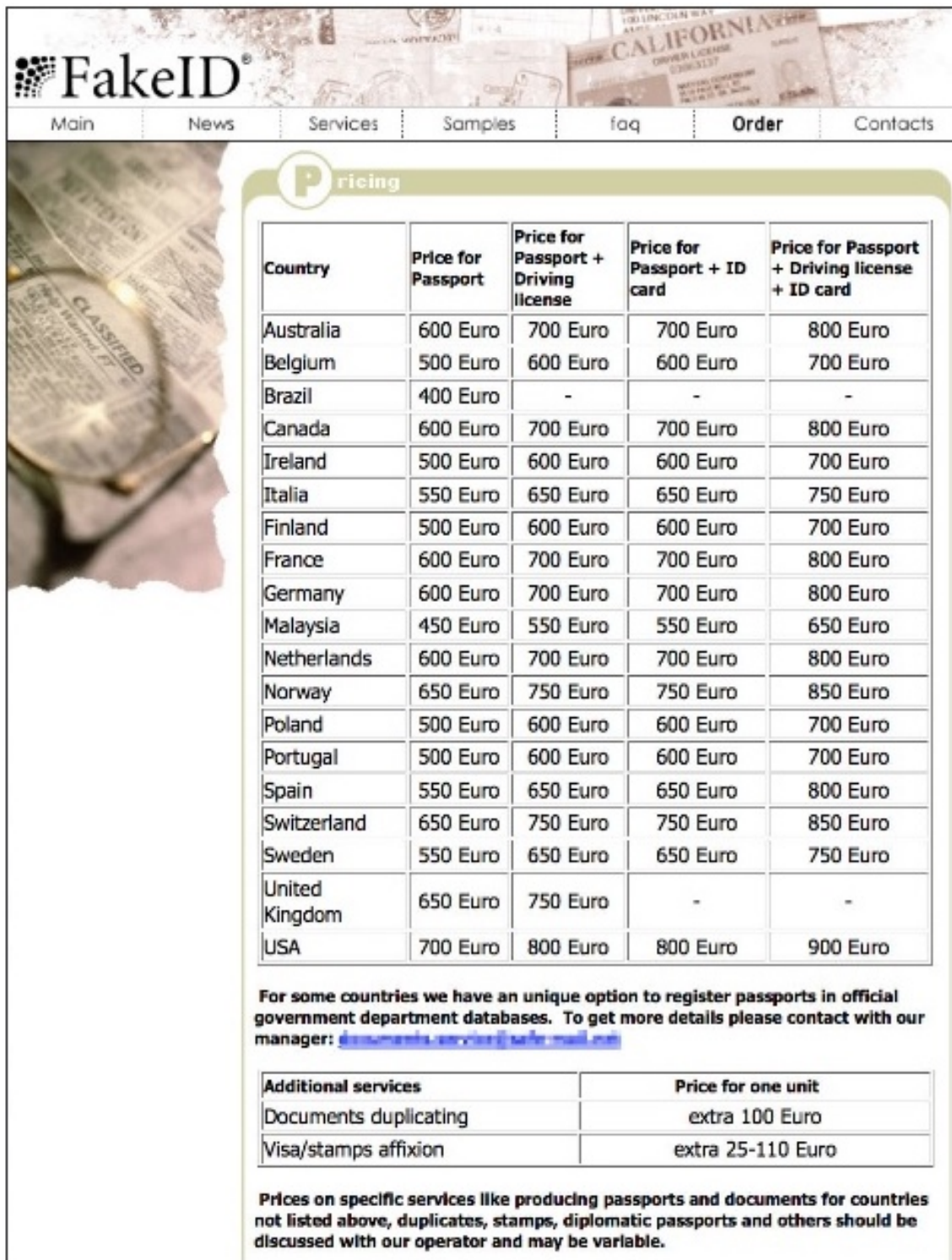
Imagem 10

Amostras de passaportes e outros documentos falsos. <sup>201</sup>

<sup>201</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 29. Texto original: Sample fake passports and other documents.



Imagem 11



**FakeID**

Main News Services Samples faq Order Contacts

### Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

For some countries we have an unique option to register passports in official government department databases. To get more details please contact with our manager: [documents.service@safe-mail.com](mailto:documents.service@safe-mail.com)


Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.


Informações sobre preços.<sup>202</sup>

<sup>202</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 28. Texto original: Pricing information.

Imagem 12



# C'thulhu



**Email:** [REDACTED]Lq4dYT1AxW7U@btmessage.ch

*Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FPL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.*

*If you're asking yourself "Why someone would need to hire a killer online?", we'll tell you: simply because it is anonymous. You can always find examples of contractors who collaborated with cops (when they were facing 20 years of prison), and you (the buyer) could end up in the prison because of that. On the other hand, you can also find examples where police found who had the interest to put out a contract, and they can come to you and you can give your testimony (which would put the hitman in jail).*

*So, it is of mutual interest to make everything anonymous. This website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins. It means we don't know you and you don't know us. We can't send you to prison, and you can't send us to prison. Of course you must take a risk when you pay in advance, but there is no interest. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face 20 years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don't contact this kind of organizations. And know, we are only one, real contractor there. Any other will try cheat you. — Contract Killer © 2011.*

No fish too big, no job too small - HITMAN does it all!

### Q & A!

**Can I see some proofs of your last work?**  
Every contract is Private, and all data is Purged after elimination proof is sent to the customer. It is Mandatory for Customer's and our Security!

**Can You give me contact to person who already used your services?**  
Again, Every contract is Private! Without Exceptions! And we will never store or share such info after completing.

**Can you give to me a good feedback about, you and some proofs of succeeded work?**  
Sorry, but no one of our happy customers stay on forums, or have time to post feedback on some trusted site. All feedbacks is written directly to our mail, and it will not show you any proof if we'll post it on our own page. And even if you'll find a feedback on an page, it was write by an random person, who don't have with as any business.

**How I would can to know that you are not a scammer as else?**  
Simply, we don't take any prepayments. We are only who ask just for proof that you have this money in your wallet, and you'll to arrange full escrow on trusted for both third party site.

Ask more, we'll add more.

We should probably get started if you'll have at least this:

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$45,000	\$90,000	\$180,000
Missing in action	\$60,000	\$120,000	\$240,000
Death in accident	\$75,000	\$150,000	\$300,000
Criple Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$12,000	\$24,000	\$48,000
Uglify	\$18,000	\$36,000	\$72,000
Two Hands	\$24,000	\$48,000	\$96,000
Paralyse	\$30,000	\$60,000	\$120,000
Rape	Low Rank	Medium Rank	High Rank and Political
Regular	\$7,000	\$14,000	\$28,000
Under age	\$21,000	\$42,000	\$84,000
Bombing	Low Rank	Medium Rank	High Rank and Political
Simple	\$5,000	\$10,000	\$20,000
Complex	\$10,000	\$20,000	\$40,000
Beating	Low Rank	Medium Rank	High Rank and Political
Simple	\$3,000	\$9,000	\$18,000

O currículo de C'thulu como assassino de aluguel.<sup>203</sup>

<sup>203</sup> CIANCAGLILI, Vincenzo; BALDUZZI, Marco; McARDLE, Robert; ROSLER, Martin. **Below the surface: Exploring the deep web.** Trend Micro Incorporated. Disponível em: [https://documents.trendmicro.com/assets/wp/wp\\_below\\_the\\_surface.pdf](https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf). Acesso em: 22 jul. 2019, p. 33. Texto original: C'thulu's resume as an assassin for hire.