João Duarte Abreu Ferreira

Compra de Drogas pela Internet

Universidade Fernando Pessoa
www.ufp.pt

Faculdade de Ciências Humanas e Sociais

Porto, 2018

João Duarte Abreu Ferreira

Compra de Drogas pela Internet

Universidade Fernando Pessoa
www.ufp.pt

Faculdade de Ciências Humanas e Sociais

Porto, 2018

João Duarte Abreu Ferreira

Compra de Drogas pela Internet

Trabalho apresentado à Universidade Fernando Pessoa como parte dos requisitos para obtenção de grau de licenciatura em Criminologia, orientado pela Professora Doutora Laura Nunes

Agradecimentos

Gostaria de agradecer a toda a Universidade Fernando Pessoa, a todos os seus professores e funcionários que demonstraram profissionalismo e muita simpatia, guardarei esta universidade na minha memória como uma excelente e enriquecedora experiência. Por mais que a experiência com todos os professores tenha sido extremamente positiva, existem duas professoras que devo mencionar aqui nos agradecimentos. Em primeiro lugar, a professora Laura Nunes, que foi a minha orientadora de estágio e que garantiu que nada me faltava para completar o mesmo, sendo muito rigorosa de forma a que os seus alunos consigam cumprir os prazos e que apresentem um relatório e projeto de qualidade, sem esquecer principalmente o facto da sua porta estar sempre aberta para atender às dúvidas ou dificuldade dos seus orientandos. A outra professora que levo uma excelente memória é a professora Lígia Afonso, que mesmo que não tenhamos mantido grande contacto durante a realização deste projeto, foi uma professora bastante competente das quais criei mais empatia durante esta licenciatura. Aproveito também para agradecer à Fundação Portuguesa "A Comunidade Contra a SIDA", por ter me acolhido no decorrer do estágio e ter sido uma experiência única e enriquecedora.

Gostaria também de agradecer aos meus país, à minha família e à minha namorada, pelo apoio dado nas melhores e piores alturas no decorrer do percurso nesta instituição e pelo seu incentivo ao meu enriquecimento académico, tenho em conta que se não fosse por eles não estaria a terminar esta licenciatura. Também a todos os meus amigos, que sempre me incentivaram a não desistir e a dar aquele puxão para conseguir terminar o curso, tal como aos meus colegas de turma, que me proporcionaram uma experiência inesquecível nesta casa.

"*Se as portas da percepção estivessem limpas, tudo apareceria para o homem tal como é: infinito*."

Aldous Huxley, "*The Doors of Perception*" 1954

Índice

Introdução

O consumo de drogas é uma realidade desde os primórdios do ser humano. Originalmente, o consumo destas substâncias estava particularmente interligado com rituais religiosos ou medicinais, e não propriamente conectado com a utilização recreativa que se assiste na atualidade. Os consumos nessa época eram comuns por diversas civilizações (Nunes, Jólluskin 2010). É possível argumentar que a vasta maioria, senão a totalidade dessas civilizações possuíssem "o seu veneno". Fosse utilizado para fins recreativos ou medicinais, esta realidade não é uma novidade para o ser humano. Por exemplo, Ötzi, que a comunidade científica estima que tenha vivido entre 3400 e 3100 A.C., o nome atribuído ao corpo extremamente bem preservado mumificado encontrado nos Alpes em 1991, tinha em sua posse em vida duas espécies de cogumelos, uma com o nome de *Fomes Fomentarius*, que não era comestível, e outra com o nome de *Fomitopsis Betulina*, que era utilizado como um medicamento natural para curar problemas intestinais, o que demonstra a utilização destes para fins medicinais à mais de 5000 anos atrás (Capasso 1998).

Dentro do espectro tecnológico, a vasta evolução que se presenciou e ainda se sente atualmente, desde a invenção do transístor em 1948 e a sua respetiva popularização nos anos 50 (Engineering and Technology History Wiki, 2015), até aos primórdios da internet e a atual IoT (Internet of Things ou Internet das Coisas) (Mancini, 2017), a sociedade adaptada-se e conforma-se de acordo com as evoluções tecnológicas. Atualmente, atividades como marcar uma viagem ou realizar uma encomenda estão a um "toque" de distância, aumentando sem duvida nenhuma o conforto e a facilidade de executar estas tarefas. Todavia, esta mudança de paradigma de modo de vida não se aplica apenas a atividades inofensivas ou juridicamente legais (Choo, Smith, McCusker 2007).

É um facto que o crime também aproveitou esta mudança de paradigma para consolidar e facilitar as suas tarefas (Emigh, 2007). Desde o malware com o intuito de afetar o sistema de outrem, ao phishing ou até ao ransomware, com a finalidade de obter ganho financeiro por parte de um individuo ou de um grupo criminoso, ou até às próprias ciberguerras financiadas por estados ou corporações, como por exemplo o worm Stuxnet, cuja criação especula-se que esteja ligada à Mossad Israelita e à NSA Americana (numa operação conjunta entre as entidades), cujo único intuito era procurar computadores ligados a sistemas de controlo SCADA, mais concretamente de dispositivos com *software* PLC da Siemens (Langner, 2011). Caso o computador não cumprisse esse critério, o vírus espalhar-se-ia no máximo até 3 outros computadores e auto-eliminar-se-ia após 3 semanas, demonstrando um ataque quase cirúrgico e extremamente bem executado, que não tinha o intuito de infetar o máximo de computadores possível, mas sim apenas o alvo pretendido, (o que não poderia ser associado a um hacker comum) para além da utilização de zero-day exploits (vulnerabilidades de um sistema que são desconhecidas pelos fabricantes e empresas de segurança informática), provando que este não vírus informático comum (Langner, 2011). Em 2010, o Stuxnet foi capaz de se infiltrar na Estação Nuclear de Natanz no Irão através de pen-drives, e foi capaz de destruir cerca de 1000 centrifugadoras da estação (Langner, 2011). Outro exemplo atual foram os ciberataques de Dezembro de 2015 na Ucrânia, que foram capazes de desligar remotamente 30 subestações elétricas e deixar 230 mil pessoas sem eletricidade durante 6 horas. Este ataque foi responsabilizado pelas autoridades à Federação Russa (Lee, Assante, Conway 2016).

O universo da droga não é uma exceção a este fenómeno. Se existe ferramentas que permitem facilitar a aprendizagem, o estabelecimento de contactos e a venda e compra de bens, é possível deduzir que eventualmente essa ferramenta possa ser utilizada para outros fins. Da mesma forma que tornou-se mais cómodo para um "cidadão comum" encomendar por exemplo uma t-shirt, não será mais cómodo também para um revendedor ou o próprio consumidor de uma droga utiliza-la também para obter esse bem? Semelhante à mesma forma de como surgiram as grandes plataformas de venda online como o Amazon ou o Ebay e grandes redes sociais como

o MySpace ou o Facebook, também surgiram nos cantos mais discretos da internet grandes plataformas de venda dedicadas a produtos de teor legal questionável, desde drogas a armas (Christin, 2012), como também surgiram redes sociais com a mesma finalidade e também facilitar a comunicação e aprendizagem entre vendedores e compradores, de forma a conseguir contornar os esforços das autoridades de combate às suas atividades (Jardine 2015).

Capítulo I - Enquadramento teórico

1.1 Conceitos Básicos – Droga e Crime/Cibercrime

De acordo com a Organização Mundial de Saúde, o conceito de droga é um termo com uma utilização variada, pois pode ser utilizado com uma finalidade medicinal ou recreativa. Dentro do panorama medicinal, a droga pode ser entendida como uma substancia com o potencial de prevenir ou curar uma doença, tal como pode melhorar o desempenho físico ou mental de um individuo. Todavia, o uso mais comum do termo "droga" refere-se às drogas psicoativas, ou aquelas que são ilegais nos termos da lei. Nestes casos, a utilização destas substancias não tem uma finalidade medicinal, mas sim recreativa. Porém, existe a utilização de drogas sem a intenção medicinal, e num quadro perfeitamente legal no ponto de vista jurídico, como é o caso do álcool, da cafeína ou do tabaco. Todavia o abuso de substâncias psicoativas pode levar à toxicodependência, que podemos definir como um estado de intoxicação crónica ou periódica, provocada pelo repetido consumo de uma droga de forma voluntária (Pinto-Coelho 1998). Este fenómeno ainda pode manifestar-se em 3 aspetos: um desejo invencível e compulsivo de continuar a consumi-la e obtê-la por todos os meios possíveis, uma tendência para aumentar a dosagem da substância que é consumida à medida do tempo, graças ao aumento da tolerância devido a estes consumos repetidos e por ultimo, a dependência física e psíquica aos efeitos da droga (Pinto-Coelho

1998). Também é possível argumentar que a toxicodependência e o crime "andam de mãos dadas", tal como a vitimação ou outros comportamentos ditos desviantes (Nunes, Sani 2014), onde a sua dissuasão e prevenção é crucial.

O conceito de crime pode ser entendido como um facto, exprimido não só através da vontade mediante uma ação ou uma omissão, como também pelo seu resultado, de acordo com Hungria (1978) (cit. In Eleutério, 2006). Dentro de uma perspetiva sobre o crime diferente da anterior, mais focada sobre o caráter legal, Ihering definiu o crime como um comportamento que lesa ou coloca em perigo um bem jurídico que se encontra protegido pela lei. Todavia, o conceito paradigmático de crime surgiu através jurista alemão Ernst Von Beling, que através da sua obra "Die Lehre vom Verbrechen" (em português "A Teoria do Crime" de 1906) e "Die Lehre vom Tatbestand" (em português "A Teoria do Tipo" de 1930) definiram aquela que é visto ainda hoje o conceito de crime, sendo este toda a ação ou omissão, típica, anti-jurídica e culpável (cit. In Eleutério, 2006).

O conceito de cibercrime é defendido pela organização não-governamental Computer Crime Research Center como a concretização de um crime utilizando tecnologias eletrónicas como meio (Cit. In Rechtman, 2017). Este crime pode-se tratar por exemplo de roubo de informações à destruição dos mesmos, permitindo também o roubo de identidade, o stalking, o cyberbullying, entre outros (Cit. In Rechtman, 2017). Todavia, o cibercrime está evoluindo não só como uma ameaça para um indivíduo, como também evoluiu nos últimos anos para uma ameaça nacional, ameaçando interesses estatais, como também apresenta uma séria ameaça para os interesses comerciais, dentro do panorama empresarial e comercial, de acordo com o Department of Homeland Security dos Estados Unidos da América (sendo este o departamento responsável pelos interesses de segurança interna norte americanos) (Cit. In Rechtman 2017). O mesmo autor destaca o surgimento de um novo campo cibernético, o "cyberinsurance", que de forma breve, pratica as mesmas atividades de uma seguradora, mas no universo cibernético, permitindo às empresas no geral

salvaguardarem os seus bens digitais através de um seguro. É importante ressalvar que para proteger os interesses, sejam pessoais ou empresariais, é importante manter um backup atualizado de todos os documentos e informações do mesmo, ou seja, um arquivo onde caso os bens digitais de alguém estivessem ou foram colocados em risco, permite sempre ter esses mesmos arquivos importantes guardados noutro local (Rechtman, 2017).

De acordo com Hale (2002), o cibercrime enquadra-se em 3 categorias. Em primeiro lugar, temos o computador como o alvo de uma atividade criminal, como por exemplo os casos de sabotagem informática ou de ciberespionagem. Posteriormente o computador como uma ferramenta para ser utilizada na execução de um delito, onde é possível exemplificar casos como as fraudes informáticas, a pirataria, o stalking ou a dissimulação de pornografia infantil. Por último, o computador como um aspeto incidental para o crime. O mesmo autor realça este campo como uma nova realidade e a maior utilização das tecnologias por parte de serviços básicos da sociedade, como as telecomunicações, transportes, fornecimento de serviços, entre outros, que dependem cada vez mais de computadores e da sua conexão à internet para o seu bom funcionamento. Da mesma forma que estes serviços estão dependentes da sua conexão à internet, o cibercrime também encontra-se bastante dependente desta. Em 2002, aquando a realização da sua publicação, o autor realçou que o cibercrime era uma problema global que custaria cerca de 50 biliões de dólares anualmente (Hale, 2002). Porém, visto que os números dados por Hale são do ano de 2002, 16 anos depois é possível afirmar que este número subiu drasticamente. Graças ao crescimento exponencial das novas tecnologias e a maior dependência da sociedade à internet.

Outra perspetiva para compreender o fenómeno do cibercrime é aquela que nos é abordada por Gordon e Ford (2006), que divide este em duas categorias distintas, Cibercrime de Tipo I e Cibercrime de Tipo II, muito semelhante à perspetiva de Yarr (2005), que distinguiu este fenómeno através de duas classificações, o cibercrime "focado no computador", o correspondente para Gordon e Ford de Cibercrime de

Tipo I, que pode ser compreendido como aquele de natureza e vertente tecnológica, como por exemplo o ransomware, que encripta o disco de um computador e exige um resgate monetário para restaurar os documentos (Liao et alii, 2016). Neste tipo de cibercrime, é notória a utilização de meios sofisticados para realizar o ato, destacando-se para além do ransomware, técnicas como o acesso não autorizado a um sistema (hacking), ciberespionagem, cibersabotagem, criação de botnets, desenvolvimento e propagação de softwares maliciosos (worms, trojans, vírus, etc) (Gordon, Ford 2006; Jewkes, Yar, 2010; Harper, Frailing, 2010; cit in Nasseri, 2014).

Quanto à outra distinção, trata-se do cibercrime "assistido por computador", o correspondente ao Cibercrime do Tipo II na perspetiva de Gordon e Ford, que consiste numa vertente de maior interação humana, aplicando-se por exemplo no roubo de identidade ou a dissimulação de pornografia infantil. Seria neste tipo que se enquadraria a compra e venda de drogas utilizando a internet como meio para alcançar um fim criminal (Jaishankar, 2011).

De acordo com Jaishankar (2011), à medida que a tecnologia evolui, como consequência de tal, é natural o surgimento de novos géneros de cibercrime, logo é fundamental compreender este fenómeno como uma temática que se encontra em constante evolução e adaptação (Cit in Nasseri, 2014).

De forma a poder diferenciar crime de cibercrime, a Cyber Security Malaysia argumenta que ambos incluem uma conduta, seja de ação ou de omissão, que por sua vez apresenta uma violação da lei. Algumas das atividades cibercriminais são na verdade atividades criminais tradicionais que já eram praticadas, porém agora dentro de novo contexto, como por exemplo a intrusão, a fraude, roubo, difamação, entre outras, mas que todavia introduziu novas espécies de condutas criminais, tais como o hacking, o phishing, o o cyberstalking, entre outras (Cyber Security Malaysia, 2011).

A mesma instituição defende que a diferenciação entre o crime e o cibercrime passa pela conduta adotada para infligir o dano, ou seja, a utilização de tecnologias para conseguir realizar a conduta criminal (Cyber Security Malaysia, 2011). O motivo para a preferência da utilização do ciberespaço ao invés do crime comum passa por vários motivos, tal como a possibilidade de anonimato dos criminosos, que podem utilizar identidades falsas ou roubadas, tal como têm a possibilidade de alterar o seu IP que lhes está atribuído para outro IP de outros país, dificultando o trabalho das autoridades em rastrear a origem. Alguns autores defendem que se deveria cessar o pensamento de que o cibercrime e o crime tradicional são conceitos diferentes e que não se encontram interligados (Husin Jazri 2011).

1.2 A Deep Web e ferramentas: Tor e VPN

Com o rápido crescimento tecnológico, a internet ganhou a perceção do público como uma plataforma tecnológica que permite aos indivíduos darem a sua voz e serem ouvidos pelo público, criando-se aqui uma "tecnologia construtora da democracia", que serve de uma ferramenta progressista e enriquecedora (Barratt et alii, 2013, Leaning, 2009, cit in Nasseri 2014). Porém esta acarreta consigo os seus efeitos nocivos, que expõem os indivíduos a diversos riscos, o que deve ser compreendido para a criminologia como uma inovação criminal, tal como um campo atual de estudo importante, que incluí uma variedade de novos tipos delitos, como também da metodologia utilizada para os completar (Nasseri, 2014).

Anteriormente foi mencionado a possibilidade de um indivíduo mascarar a sua identidade e até conseguir alterar o seu IP e país de origem. Isto é possível com a utilização de um VPN, ou Virtual Private Network (Microsoft, 2001). Com a utilização desta ferramenta não é só possível mascarar a identidade de um individuo às autoridades, como também é possível mascarar o tráfego ao ISP (Internet Service

Provider, por exemplo as empresas contratadas por um individuo para o fornecimento do serviço de internet), e aceder a websites bloqueados pelo ISP por ordem judicial (um exemplo nacional é a utilização de VPN's para aceder a websites de streaming como o Tugaflix, que se encontra barrado por ordem judicial, ou o caso mediático do The Pirate Bay). Porém a utilização do VPN não se restringe apenas a atividades de caráter legal duvidoso, em muitos casos são utilizados por dissidentes e críticos políticos de regimes com uma forte censura na internet, como o caso de países como a Bielorrússia, a Coreia do Norte, Paquistão, Arábia Saudita, entre outros (Freedom House, 2017).

Porém o exemplo mais mediático de controlo estatal sobre a internet é o caso da China. As autoridades chinesas possuem um fortíssimo controlo sobre a internet, que aquando a abertura do país à mesma e à introdução à economia de socialismo de mercado, foi criada o que conhecemos por "Great Firewall of China", ou a Grande Firewall da China, sendo este nome uma óbvia amálgama entre a firewall e a Grande Muralha da China, que pretende manter de fora as ameaças cibernéticas ao seu regime. Para combater tal ameaça e salvaguardar os ideais e interesses do estado, foi criada a "Grande Firewall da China" (Clayton, et alii, 2006). Esta firewall utiliza vários métodos, como o bloqueio de IP's, a filtragem e redirecionamento de DNS ou URL's, a filtragem de pacotes, entre outros métodos. Para conseguir ultrapassar esta "muralha" existem várias possibilidades, entre as quais a utilização de proxys, a utilização de browsers onion, como o caso do Tor, o uso de VPN's, entre outros métodos (Freedom House, 2017).

Para compreender os VPN's é necessário compreender e saber diferenciar uma rede privada de uma rede pública. Uma rede privada trata-se de dois ou mais computadores interligados que formam uma rede entre si, ou network, que ao partilharem informações tornam-se numa LAN (Local Area Network), cujas ligações são efetuadas através de hubs ou switches (Silva, 2008). No caso de uma rede pública, trata-se de um compartilhamento de tudo entre todos os conectados, como por

exemplo a internet, que interliga vários computadores e indivíduos, que é um bom exemplo do que é uma rede pública, sem um dono da informação ou administrador a tomar conta da rede. Ora, o VPN surge como uma tentativa de criar uma rede pública e utiliza-la como se fosse uma rede privada com segurança ao criar um "túnel" entre ambos os computadores e mantendo o seu tráfego anónimo e impossível de determinar pelas ISP's (Silva, 2008).

Os websites de compra e venda de droga online que serão abordados neste projeto, encontram-se na denominada dark web, que por sua vez está incluída na deep web (Martin, 2013). Muitas vezes, as pessoas são induzidas em erro e consideram a dark web e a deep web ser a mesma coisa, todavia este pensamento não está correto (Berthier and Cukier, 2008; Bethencourt et al., 2007; Bailey et al., 2006, cit in Nasseri, 2014). A forma mais fácil de compreender como funcionam estas camadas é em dividir a internet em 3 partes. A surface web, a deep web e por ultimo, a dark web (Daga, 2017).

A surface web compõe 4% da internet, e consiste em todos aqueles websites que se encontram indexados, ou seja, que conseguimos aceder através do nosso motor de busca comum, como o Google ou o Yahoo. Alguns exemplos de websites que se encontram nesta camada são por exemplo o Facebook, o Gmail ou até o próprio website da Universidade. Esta podemos classificar como a uma internet que está ao alcance de qualquer um. Porém é surpreendente o facto que esta apenas compõe 4% da totalidade da internet, e estamos a referir virtualmente todos os websites que nos podem surgir num motor de busca como o Google (Daga, 2017).

A deep web por sua vez compõe a maior parte da internet, cerca de 96% da mesma. Esta consiste em websites não indexados, ou seja, que não são possíveis de alcançar através do motor de busca comum (Wright, 2008; King, 2004, cit in Nasseri, 2014). A

larga maioria da deep web trata-se de bases de dados, recursos governamentais, documentos, registos, diretórios, etc (Wright, 2008; King, 2004, cit in Nasseri, 2014). Também inclui páginas que são utilizadas pela maioria dos navegantes da internet, como webmails e contas bancárias, como também consiste em serviços pagos, como serviços de streaming. A atividade ilegal na deep web é bastante incomum tal como na surface web. Para alcançar esta camada não é necessário um browser onion como o Tor, pois esta pode ser acedida com os browsers comuns como o Explorer, Mozilla ou Chrome, porém, sem o link é impossível de aceder à página. Muitos websites, de caratér legal, fazem questão de se manterem não indexados de forma a manterem os "curiosos" fora da página (Daga, 2017). Um exemplo simples de compreender a deep web é o seguinte, um aluno universitário por exemplo que redige um trabalho e submete-o a um serviço de cloud dos servidores da universidade. Esse serviço providenciará um link que permite aos professores ou colegas acederem ao seu trabalho, mantendo os terceiros de fora. Ou seja, caso fosse pesquisado o tema desse trabalho num motor de busca, mesmo que com palavras chaves, seria impossível aceder sem possuir o link original (Daga, 2017).

Por último temos a infame dark web. A dark web na realidade não é a deep web, mas sim uma parte dela, consistindo em cerca de 6% da deep web e da internet no geral. Esta rede foi criada com o intuito de manter o anonimato e de manter-se oculta das restantes redes. Aqui, não só os simples motores de busca como o Google, como também os browsers comuns não conseguem aceder aos seus websites (Daga, 2017). Para tal, é necessário a utilização de um browser especial, como por exemplo o mais conhecido para esta rede, o Tor, como também é possível mencionar outros serviços como o I2P, o Freenet e o Decentralized Network 42 (DN42) (Daga, 2017). Muitas páginas na dark web, para além da de requererem a utilização de um browser especial, requerem que o utilizador tenha uma conta autorizada para poder acede-los. É aqui que é possível encontrar vários serviços e atividades ilegais, todavia é errado assumir a dark web como uma rede que serve apenas para tal (Daga, 2017).

É comum utilizar uma fotografia de um icebergue para descrever este fenómeno. Ao observar um icebergue, a parte visível é muito pequena quando comparada com a parte oculta, aquela que está por de baixo da linha do oceano. Assim, dá-se o exemplo de que a internet tem muitas semelhanças com o icebergue, pois a parte visível, ou seja, a surface web, não passa de uma parte muito pequena em comparação à parte que não é visível, neste caso a deep web (Daga, 2017).

Quanto ao browser Tor, que já foi abordado brevemente neste projeto, este não passa de um browser de onion routing. Este é o browser mais utilizado e mais conhecido que utiliza esta tecnologia. Tor, por sua vez, significa "The Onion Router". Mas de que é que se trata este onion routing? O onion routing é uma infraestrutura para comunicações privadas utilizando uma via de rede pública. Este fornece conexões anónimas extremamente complicadas de analisar por terceiros. Graças a este grande nível de privacidade, este torna-se num meio muito procurado, por exemplo por dissidentes políticos, mas que todavia, devido a este caráter sigiloso, abre portas à criminalidade. Estas conexões são em tempo real e encriptadas nos dois sentidos da comunicação (Reed, Syverson, Goldschlag 1998).

De acordo com o website do Tor, esta ferramenta protege o usuário da forma mais comum de vigilância na internet, que é a análise de tráfego, que permite observar quem está comunicando com quem numa rede pública, ao analisar o payload dos dados (Tor, 2018). O Tor reduz os riscos desta análise de tráfego ao distribuir as ligações pela internet, por vários outros servidores, fazendo com que seja impossível de rastrear até a origem. Em vez de existir uma conexão direta entre os recetores, os dados são transmitidos por um percurso aleatório, passando por vários relays que ocultam a origem e o destino (Tor, 2018). O website do Tor dá nos o exemplo de alguém que vai apagando as suas pegadas de forma a não ser perseguido. Porém, o próprio Tor reconhece que não consegue salvaguardar o anonimato na integra e que este apenas se foca na proteção do transporte de dados (Tor, 2018). É realçado que todo o utilizador deve ter atenção, particularmente às informações que partilha online,

tal como sublinha a importância do bom senso enquanto navegando na internet (Tor, 2018).

O website do Tor também menciona aqueles que utilizam o Tor com bons intuitos. São destacados, por exemplo, os simples civis que apenas pretendem manter as suas comunicações privadas ou que pretendem pesquisar temas delicados na internet, como também existem aqueles que o utilizam com o intuito de ultrapassar a censura (Tor, 2018). Outros exemplos que nos são dados são os jornalistas, onde destacam os Reporters Without Borders ou os jornalistas chineses que utilizam o Tor como uma ferramenta de liberdade de expressão, como também mencionam ativistas e whistleblowers (denunciantes, por exemplo Julian Assange ou Edward Snowden), que utilizam esta ferramenta para denunciar determinadas situações, com um intuito positivo (Tor, 2018). As autoridades e os militares também são mencionados na sua lista, particularmente por utilizarem o Tor para realizar vigilância online, operações encobertas, ciberespionagem ou simplesmente criar um canal seguro para vítimas ou testemunhas de um delito poderem realizar uma denúncia de forma anónima (Tor, 2018). Por ultimo são mencionados os empresários, que podem vir a necessitar de utilizar um canal seguro e encriptado para o desempenho das suas funções, tal como os peritos informáticos, que por motivos profissionais necessitam de recorrer a esta ferramenta regularmente (Tor, 2018).

Não obstante, o Tor reconhece que existem pessoas que utilizam esta ferramenta com fins menos propícios e que não concorda com tal. Porém, a página do Tor argumenta que para além dos criminosos terem atualmente meios mais "atualizados" que esta ferramenta, o anonimato que lhes atraí a browser permite também que o cidadão comum possa ter uma maneira não só de se manter anónimo, como também de combater o roubo de identidade e o stalking, por exemplo (Tor, 2018).

1.3 A ideia de Criptomoeda

O termo de criptomoeda surgiu originalmente em 2008, num paper que se encontrava assinado sob o pseudónimo de Satoshi Nakamoto, a quem é atribuído a "invenção" da bitcoin. A critpomoeda pode ser considerada como "um bem digital construído como meio de troca, com base na tecnologia da criptografia, para garantir o fluxo transacional, bem como para controlar a criação de unidades adicionais da moeda" (Chohan cit In Marinho, Ribeiro, 2017). Alguns exemplos de criptomoedas são, o Bitcoin, o Ethereum, Litecoin, Dogecoin, entre muitas outras. O governo venezuelano por exemplo, criou este ano uma criptomoeda denominada de Petro (El Petro 2018).

Estas moedas têm por base de funcionamento uma inovação tecnológica chamada de blockchain, que surgiu em 2008 juntamente com o Bitcoin, como um registo comum público de transações. O blockchain, também conhecido por Distributed Ledger Technology, tem a capacidade de diminuir ou até de terminar com a necessidade de qualquer intervenção centralizada, intermediária ou estatal, utilizando mecanismos criptográficos que alcançam um consenso entre registos digitais (Marinho, Ribeiro, 2017). Marinho e Ribeiro afirmam que podemos considerar esta tecnologia como um sistema de banco de dados distribuídos, que funciona como um instrumento de registo ao permitir a transparência de valores e informação, sem a necessidade de uma autoridade de validação, sendo esta feita por P2P (peer to peer) (Marinho, Ribeiro, 2017). Desta forma, todas as transações utilizando, por exemplo, a bitcoin são públicas e acessíveis a todos, sendo possível determinar ambas as contas da transação, como também o montante envolvido, porém, é difícil associar uma conta a alguém sem saber a sua chave (Marinho, Ribeiro, 2017).

A tecnologia do blockchain tem por base quatro argumentos. O registo compartilhado de transações (o ledger), o consenso para verificação de transações, um contrato que

determine as regras de funcionamento e por ultimo, o mais fundamental, a criptografia (Marinho, Ribeiro, 2017). Nesta rede, as informações apenas são acrescidas ao registo digital (ledger) quando existe consenso entre as partes. Para verificar este consenso entre as partes, existe um processo de validação, feito por participantes da rede chamados de nós ou peers, processo chamado de mineração. Esta mineração é realizada de uma forma democrática, de acordo com Marinho e Ribeiro, e consiste na resolução de problemas matemáticos através de uma competição entre os participantes em rede, onde o computador que for capaz de resolver o problema atribuído, é remunerado pela sua resolução com uma percentagem da transação efetuada (Marinho, Ribeiro, 2017). O primeiro bloco minado desta rede, pelo próprio Nakamoto, valia cerca de 50 bitcoins, porém, este valor está programado a diminuir com o tempo de forma a que o número total de bitcoins em circulação não ultrapasse os 21 milhões. Esta área da mineração tornou-se em um negócio, particularmente na China, onde encontram-se instalações com equipamentos de processamento especializados para a mineração de bitcoins, chamados de mining pools (Johnson, 2014).

Existem ideias de que o blockchain poderá influenciar bastante o nosso estilo de vida, devido às suas propriedades de confidencialidade, transparência e descentralização. Alguns teorizam que esta tecnologia poderá ser implementada por exemplo no sector jurídico, ou até no próprio ato de voto ou emissão de certificações e registos (Sandre, 2016). Todavia, esta tecnologia é relativamente recente, com apenas 10 anos, não é possível imaginar para já a implementação desta ferramenta nesses sectores sociais.

A bitcoin começou a ser desenvolvida em 2007, por um autor sob o pseudónimo de Satoshi Nakamoto e foi lançado ao público, em Janeiro de 2009. Esta foi a primeira criptocurrencia, que para além da sua confidencialidade e transparência, permitia a realização de pagamentos internacionais (Business Insider, 2017).

De acordo com Ulrich (2014), não podemos considerar a bitcoin como uma moeda de um ponto de vista legal, porque não é emitida nem definida por um estado. Podemos considerar o bitcoin no âmbito financeiro como uma espécie de ativo especulativo, tal como o ouro, que possui um valor flutuante, e que oscila de acordo com a procura e a demanda. Ulrich (2014) argumenta que no fundo podemos considerar o bitcoin como uma commodity, ou comodidade, que de acordo com o Commodity Exchange Act dos Estados Unidos da América, pode ser qualquer produto ou mercadoria, e, mesmo que digital, podemos considerar o bitcoin como uma nova classe de ativos, neste caso de moedas digitais, ou uma comodidade digital. Para tal, o autor argumenta que o bitcoin é um ativo próprio e que deve ser enquadrado numa nova classe onde os ativos compartilham caraterísticas tanto das moedas comuns como das comodities (Ulrich, 2014).

Do ponto de vista técnico, as moedas virtuais transferem-se através de transações entre o endereço do destinatário e do remetente utilizando a internet. Essas endereços são as chaves públicas das suas carteiras virtuais, composto por 27 a 34 carateres aleatórios, em linguagem alfanumérica case-sensitive, ou seja, sensível a letras maiúsculas ou minúsculas (Cabral, 2013). Um exemplo de endereço é o seguinte: 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX (este é o endereço que contém as bitcoins apreendidas pelas autoridades ao Silk Road).

O processo é simples, o utilizador recebe o endereço para quem tem que enviar as moedas, cria uma transação e esta é transmitida (Bitcoin, 2008). Todas as transações são públicas e acessíveis, porém como os nomes das contas são letras e números aleatórios não associados a qualquer entidade, é difícil determinar o verdadeiro utilizador da conta. A carteira do utilizador armazena as informações e credenciais necessárias para realizar as transações, como a sua chave. A tecnologia da bitcoin usa um sistema criptográfico com 2 chaves, a chave pública e a chave privada (Bitcoin, 2008). A chave pública, como o nome indica, é a chave que pode ser partilhada para com o público e serve para receber fundos. A chave privada por sua vez, é pessoal e

não deve ser partilhada, pois esta é a responsável pelo acesso à conta e serve para assinar digitalmente a transação. Sem esta chave é impossível transferir bitcoins, tornando a conta inutilizável, pois não existe nenhuma outra maneira de aceder à mesma (Bitcoin, 2008).

Abordando o fundador do bitcoin e a quem é atribuída a invenção da tecnologia de blockchain, Satoshi Nakamoto começou a trabalhar neste projeto em 2007, anunciou o mesmo em 2008 e no ano seguinte lançou publicamente a bitcoin, em open source, ou seja, com o código acessível para todos, de forma a que outros também pudessem contribuir para melhorar o sistema ou corrigir alguma eventual falha (Wallace 2011). Em Abril de 2011, Nakamoto anunciou por via email a um colaborador da bitcoin que partiu para novos projetos, e desde então nunca mais publicou com a sua conta nos fóruns de bitcoin, desaparecendo totalmente da rede. O seu nome na realidade é um pseudónimo, e a identidade real do criador da bitcoin é alvo de muita especulação (Wallace 2011). Alguns dos nomes que os media e os internautas afirmam ser a verdadeira identidade de Nakamoto são, Hal Finnley, cientista informático perito em criptografia, que foi o primeiro individuo a receber uma transação de bitcoins, de Nakamoto; outro nome é Nick Szabo, entusiasta de redes monetárias descentralizadas (Wallace 2011). Até o próprio Elon Musk, responsável pela Tesla e SpaceX, foi acusado de ser o responsável, o que veio posteriormente veio a negar (Bernard 2017). A lista de indivíduos que se são alvo de especulação de serem a verdadeira pessoa por detrás de Satoshi Nakamoto prolonga-se, porém será impossível determinar a sua verdadeira identidade, a não ser que seja por vontade deste e que apresente a sua chave da carteira bitcoin (Bernard 2017). Esta especulação é natural, visto que Nakamoto realizou as primeiras minerações da moeda. Como a mineração de bitcoins está programada para diminuir o valor ao longo do tempo, as primeiras minerações tinham um valor altíssimo comparado com os valores atuais. Visto que foi o primeiro individuo a minerar e manteve-se durante os primórdios desta moeda virtual a fazer tal atividade, especula-se que a sua "fortuna virtual" esteja avaliada em 1 milhão de bitcoins, que no auge da moeda, em Dezembro de 2017 quando esta quase alcançou os 20 mil dólares por bitcoin, faria de Nakamoto a 44º personalidade mais rica do

mundo, nessa altura com aproximadamente 19.4 Biliões de dólares em bitcoins (Wong, 2017).

A regulamentação da bitcoin varia de país em país (Chohan, 2017). Na maioria dos países a sua utilização é legal ou ainda não possui uma regulamentação específica sobre a mesma, com algumas exceções onde a utilização da mesma é limitada ou ilegal (Chohan, 2017). No caso da União Europeia, a bitcoin encontra-se num estado legal. Porém, a Comissão Europeia já alertou para os riscos da sua volatilidade e pondera realizar algum tipo de regulamentação ou legislação relativamente à mesma (Gillespie, 2018). Na Alemanha por exemplo, a bitcoin é isenta de impostos desde que seja utilizada como um método de pagamento (Kelso, 2018). São cada vez mais as instituições que aceitam bitcoins como método de donativo, como o Internet Archives, a Wikileaks ou a Eletronics Frontier Foundation, onde algumas empresas também começam a aceitar a bitcoin como forma de pagamento pelos seus serviços, como a Microsoft, a Dell, o PayPall ou a Steam (Cabral, 2013).

A nível nacional a moeda virtual é totalmente legal, porém não existe nenhuma legislação ou regulamentação sobre a mesma. Para Hélder Rosalino, um dos administradores do Banco de Portugal, a criptomoeda não é viável e não deve ser considerada uma moeda devido à sua volatilidade e ao risco de natureza especulativa, todavia, reconhece o seu potencial tecnológico, nomeadamente a tecnologia de blockchain (Costa, 2017). O Jornal de Negócios noticiou em 2017 que de acordo com o Ministério das Finanças, esta moeda virtual não é tributável, porém, para a Autoridade Tributária, todos os rendimentos obtidos através de uma criptomoeda devem ser tributados, mostrando uma contradição entre as instituições governamentais devido a um vazio legal e à falta de regulamentação sobre as moedas descentralizadas (Adam, 2017). O mesmo jornal avançou, com fontes da Agência Lusa, que em 2018 o parlamento encontra-se a analisar uma proposta relativamente à utilização das moedas virtuais, com o objetivo de proteger os consumidores (Lusa, 2018). Esta regulamentação sobre a moeda virtual acaba por ser uma tendência

europeia com o intuito de prevenir a utilização desta tecnologia para fins de lavagem de dinheiro ou de financiamento de atividades terroristas (Pollock, 2018).

A bitcoin é criticada principalmente por causa da sua volatilidade e teor especulativo (Cabral, 2013), como também pela sua irreversibilidade, pois após uma transação ser efetuada, não é possível cancelar a mesma (Nakamoto, 2008). Porém um tema muito controverso é a atração do cibercrime a esta moeda.

Os negócios de caráter legal duvidoso existentes na dark web possuem uma característica em comum, o pagamento em moeda virtual, visto que a confidencialidade entre ambas as partes é um interesse mútuo (Cabral, 2013). O crime organizado também é particularmente atraído pelo interesse da confidencialidade, nomeadamente para realizar esquemas de lavagem de dinheiro (Pollock, 2018).

Em 2011 surgiu um cavalo de Troia cujo nome atribuído foi de infostealer.coinbit, e o seu único intuito era infiltrar-se em sistemas, procurar carteiras digitais e transferir a chave das mesmas para o seu criador (Doherty, 2011). Os ransomwares por exemplo, exigem um pagamento em criptomoeda de forma a não ser possível rastrear a identidade do recetor das moedas (Liao et alii, 2016). Na dark web, existem diversos fóruns onde é possível contratar um hacker ou comprar malware utilizando criptocurrências, entre outros serviços (Martin, 2013).

O rastreio por parte das forças de segurança torna-se num trabalho muito árduo, visto que se trata de uma rede descentralizada P2P, onde se torna complicado poder acusar alguém de ser o titular de uma determinada conta. Porém não é impossível, se o indivíduo não tomar certas precauções, como por exemplo esconder o seu IP de origem através de um VPN (Nasseri, 2014).

A atração do mundo criminal para esta moeda não pode, nem deve, ser ignorado. Desde um criminoso que esteja a trabalhar por conta própria ou um grupo criminal bem estruturado, é verdade que enquanto este tipo de moeda existir, este universo aproveitará-se dele. Os esquemas de lavagem de dinheiro são uma das atividades criminais principais que usam a moeda virtual como meio, o que leva a uma grande atenção por parte das autoridades, mas não é este a única preocupação das mesmas (Reynolds, Irwin, 2017). O financiamento de grupos terroristas utilizando esta moeda tem se tornado cada vez mais numa realidade, onde o investidor garante o seu anonimato, tornando extremamente complicado para as agências de autoridade de alcançar o agente financiador (Reynolds, Irwin, 2017).

Neste capítulo, o termo bitcoin foi utilizado diversas vezes, porém, o mesmo se sucede nas outras moedas virtuais. Graças ao crescimento e à fama exponencial desta moeda ao longo dos anos, mais o facto desta ser de livre acesso a todos na internet, novas moedas virtuais foram surgindo ao longo do tempo, influenciadas pela bitcoin (Wallace, 2011). Podemos destacar a segunda criptomoeda mais popular, a Ethereum, fundada em 2014 por Vitalik Buterin, uma criptomoeda que não pretende explorar o campo da tecnologia blockchain apenas em moedas virtuais, onde já é possível a realizar contratos inteligentes utilizando esta tecnologia (Ethereum, 2018). Outros exemplos de moedas virtuais são a Litecoin, a Dogecoin, entre outras. A Potcoin por exemplo, é uma moeda virtual inventada com o propósito de ser utilizada na crescente indústria americana da cannabis, onde pretende ser a solução de moeda digital para este ramo empresarial (Potcoin, 2018).

1.4 Porque e como comprar drogas online?

Os principais fatores que despertam interesse em optar por adquirir uma substância ilegal por via online contra a via dita tradicional é sem dúvida a confidencialidade e a comodidade. Em vez de optar pela via tradicional, aquela onde por exemplo o usuário tem que se dirigir até ao vendedor ou vice-versa, e onde é obrigado a dar a cara, no caso dos criptomercados já não existe o transtorno de ter que se deslocar até outrem ou em ter que revelar a sua identidade (Martin, 2013 cit in Nasseri 2014). A verdade é que para além destes fatores, corta-se drasticamente também o risco de ser detetado pelas autoridades.

De acordo com Martin (2013), a definição de criptomercado pode ser entendida como "*um fórum online onde bens e serviços são trocados entre entidades cuja utilização de encriptação digital mantém o anonimato das suas identidades*" (cit in Nasseri, 2014).

Destaca-se que nestes websites o sistema de venda não saí muito à regra do que é o do Ebay ou do Amazon (Pauli, 2012; Ormsby, 2012; cit in Martin, 2014). Ambos estes serviços legais e ilegais possuem a característica de poder atribuir feedback a um vendedor após uma compra, o que permite ao vendedor receber mais prestigio no site e eventualmente mais clientes, como permite também aos utilizadores saberem se estão a lidar com um individuo "sério" ou se é um individuo suspeito (Martin, 2014). Isto permite diferenciar facilmente quais são os vendedores legítimos e analisar as suas normas de trabalho, tais como a qualidade da substância, a sua embalagem e dissimulação, entre outros aspetos à vontade do utilizador que queira avaliar (Martin, 2014).

Todavia, Martin (2014), alerta para a má-interpretação da linguagem para descrever estes mercados, nomeadamente a associação entre criptomercados e as grandes superfícies comerciais online, como o Ebay e o Amazon. Os mass media tendem a descrever os criptomercados desta forma, mesmo que a "mecânica" por de trás do seu funcionamento seja semelhante, a comparação com estes colossos da internet serve apenas para criar pânico entre as pessoas, como também para passar uma imagem negativa e incapaz das autoridades (Nasseri, 2014).

Sucintamente, podemos concluir que os fatores essenciais que tornam este fenómeno tão atraente são nomeadamente a confidencialidade e o conforto, porém não obstante o profissionalismo e a maior variedade de produtos e de vendedores, tal como as interfaces simples e semelhantes a mercados virtuais legais, e a capacidade de contorno às autoridades (Martin, 2014).

O método de compra é relativamente simples, tal como no Ebay, envia-se uma mensagem a um determinado vendedor e demonstramos interesse num determinado produto. O vendedor pede o valor em dólares e este é enviado sob a forma de uma criptocurrência, da carteira virtual do website do comprador para a do vendedor. Este processo será explicado com maior detalhe quando o Silk Road e outros criptomercados forem abordados, mas é possível realçar que a utilização da carteira no próprio website deve-se ao facto do website retirar uma pequena percentagem de transação, por ser o intermediário entre ambas as partes (Martin, 2014).

Porém alguns criptomercados não limitam o seu negócio apenas a drogas. Mesmo que o modelo de negócio seja mais focado nos anúncios de substâncias ilegais, alguns criptomercados aproveitam-se da sua tecnologia e facilitam indivíduos a adquirirem outros bem ilegais, tal como armas ou pornografia (Christin, 2012). Todavia, os estudos conduzidos por Van Hout e Bingham (2013), revelam que na realidade,

muitos criptomercados rejeitam outros tipos de actos ilegais. O Silk Road, por exemplo, proibia qualquer anuncio de natureza ilícita, exceto o comércio de drogas, onde material como pornografia infantil ou documentos falsificados eram completamente proibidos (Cit in Nasseri, 2014).

O Observatório Europeu da Droga e da Toxicodependência (2015) afirma que o crescimento deste tipo de mercados virtuais apresenta um desafio para as autoridades. Por sua vez, a EUROPOL afirma que as autoridades europeias ainda não conseguiram entender este fenómeno na totalidade, nem como conseguiram desenvolver uma estratégia eficaz de os erradicar (Décary-Hétu, Giommoni, 2017).

1.4.1 O caso do *Silk Road* e outros criptomercados

O Silk Road é sem dúvida o caso mais mediático deste tipo de criptomercados, utilizando a internet como meio, serve-nos de um excelente exemplo de como as novas tecnologias e as técnicas de encriptação estão a alterar o panorama criminal e a nossa perceção sobre o mesmo, revelando ser uma inovação criminal. Porém o Silk Road não foi um dos primórdios deste fenómeno, esse titulo pertence originalmente ao The Farmer's Market, lançado em 2006 e encerrado em 2012 (Nasseri, 2014).

Estes serviços, porém abordando em particular o Silk Road, oferecem um mercado mundial e oferecem informações sobre os produtos, tal como confidencialidade entre as partes (Barratt et alii, 2013). Este opera no lado encriptado da internet, na dark web, onde para aceder é necessário a utilização de um browser como o Tor (Nasseri, 2014). Martin afirma que este é um caso de um criptomercado, um conceito novo e recente de cibercrime, e não de um simples cibermercado, pois apresenta características que protegem e garantem o anonimato dos seus utilizadores, o que lhes

permite comunicar, consumir, produzir e disseminar material uns com os outros (Martin, 2014). O mesmo autor realça que de qualquer das formas este serviço possui várias fases, como ofensas criminais, ambas online e offline, como também por outro lado apresenta uma alternativa muito menos violenta comparada ao tráfico convencional, mas sem esquecer que é necessário ter em atenção que os criptomercados são um fenómeno relativamente recente e largamente desconhecidos, que na sua perspetiva são necessários mais estudos e análises para poder chegar a uma conclusão definitiva (Martin, 2014).

O Silk Road na sua essência não é um serviço que pretende servir de intermediário apenas para a compra e venda de drogas, pois oferecia outros serviços ou itens ilegais. Todavia as suas ofertas são principalmente sobre drogas, enquanto que os restantes compõem apenas uma pequena fatia do website (Decary-Hetu, Aldridge, 2014).

Para efetuar uma compra ou venda, é necessário registar-se em primeiro lugar. Depois, no caso de vendedor, deve fazer um anuncio do produto que está a vender, colocar as informações do mesmo e aguardar por um contacto. O comprador, por sua vez, após encontrar o produto desejado, deve comunicar com o vendedor e enviar o valor necessário em bitcoin ou outra moeda virtual para a sua carteira digital do website. Após receber a moeda virtual na carteira do website, o utilizador pode proceder ao ato de compra (Nasseri, 2014).

Tal como é comum nos outros mercados deste género, este oferecia um sistema de proteção que salvaguardava os interesses do consumidor. Após o valor acordado em moeda virtual ser transferido, este não parte logo diretamente para o vendedor, permanece com o website até que o comprador receba a encomenda e confirme que recebeu o que estava previsto. Estes envios são feitos por via postal (Decary-Hetu, Aldridge, 2014). Caso o cliente esteja satisfeito, este confirma a entrega e o Silk Road

liberta o valor para o vendedor, tirando a sua percentagem de intermediário (Decary-Hetu, Aldridge, 2014). No caso de conflito, onde o comprador afirma que não recebeu o desejado e o vendedor insiste que enviou o produto correto, o website fica com o montante estipulado. Ambos o vendedor e o comprador após este processo podem atribuir um "feedback" mutuamente, atribuindo numa escala de 1 a 5 a sua satisfação para que os outros utilizadores do site tenham uma perceção de com quem estão lidando (Decary-Hetu, Aldridge, 2014).

Para aumentar a competitividade e oferta perante os seus concorrentes, é comum alguns vendedores realizarem promoções especiais, como de Natal ou de Halloween por exemplo, dar garantias de qualidade, fornecerem um serviço de cliente excelente e profissional, ou até garantirem a promessa de reenvio da encomenda caso intercetada (Aldridge and Decary-Hetu, 2014; Van Hout and Bingham, 2013; Martin, 2013; Christin, 2012, cit in Nasseri, 2014).

Os anúncios do Silk Road eram compostos pelo seu título, que continha o nome da droga em questão e a respetiva quantidade, uma breve descrição, a categoria do produto, o preço, os países para qual a encomenda é enviada, tal como opções no envio postal (Decary-Hetu, Aldridge, 2014).

Um potencial que este sistema online apresenta é a possível mudança sobre a perceção da tradicional guerra contra a droga, em que as suas estratégias de proibição mostram-se ineficazes, estigmatizando os consumidores e intensificando o crime e a violência, tal como demonstram-se ineficientes em conseguir terminar com estes novos mercados mais organizados e eficientes, o que revela o surgimento de uma nova geração de traficantes, dependente de tecnologias, porém extremamente discreta. (Martin 2014). Este mercado onde as transações são discretas e relativamente seguras das autoridades apresenta também menores riscos para os seus utilizadores do que o

mercado tradicional, como por exemplo o não pagamento, o roubo ou a violência (Decary-Hetu, Aldridge, 2014). Neste novo paradigma do tráfico, a comunicação e a simpatia, tal como a prestação dos serviços tornam-se mais importante do que a demonstração de força, associada ao tráfico tradicional, demonstrando um benefício para ambas as partes ao reduzir a violência subjacente aos métodos tradicionais, através da possibilidade de não existir encontro entre ambos, apenas transações (Martin, 2014; Decary-Hetu, Aldridge, 2014).

O Business Insider (2016) avança que a Colômbia, o maior produtor de cocaína do planeta, a pasta de coca, o ingrediente principal da cocaína, teve um aumento de 44% na sua cultivação em 2015. Com fortes medidas de proibição do cultivo da planta de coca e operações conjuntas entre as autoridades colombianas e americanas, o fenómeno não parece estar a abrandar. Isto ocorre devido às posses e à classe social dos cultivadores, onde não lhes é rentável plantar colheitas legais, como vegetais ou frutas, mas sim produzir pasta de coca. Porém, a mesma fonte avança que mesmo sendo esta a colheita mais rentável na Colômbia, o simples fazendeiro recebe apenas 1000 dólares por ano em média, o que lhes permite apenas sobreviver no limiar da pobreza (Business Insider, 2016). Em alguns casos chega ao extremo dos cultivadores trocarem a pasta de coca por alimentos e outros bens essenciais, o que demonstra que estes indivíduos não recebem os "grandes créditos" do tráfico de droga, e apenas o fazem por necessidade e sustento. Para fabricar um quilo de cocaína pura é necessário aproximadamente uma tonelada de folhas de coca frescas. Uma tonelada dessas folhas custa à volta de 400 a 500 dólares na Colômbia, enquanto que o produto final, um quilo de cocaína pura, custa cerca de 150 mil dólares nos Estados Unidos da América, segundo a agência Reuters, citada pelo Business Insider. Para além do crime organizado, as FARC, (Forças Armadas Revolucionárias da Colômbia) durante a sua atividade terminada em 2017, promoviam o cultivo pelos camponeses tal como protegiam-os das autoridades e taxavam a sua produção para financiar as suas atividades (Business Insider, 2016).

Este fenómeno demonstra que a maioria do lucro envolvido no negócio fica com o intermediário. Os fazendeiros, com fracas condições de vida, responsáveis pela colheita desta matéria e transformação, são na verdade quem menos lucra com este trabalho. As grandes percentagens da produção ficam na mão de grupos criminais ou terroristas, como os cartéis mexicanos ou as FARC. Mas este fenómeno não se aplica apenas à cocaína (Business Insider, 2016). No Afeganistão, um quilo de heroína rende 163 dólares a um agricultor, enquanto que o produto refinado vale pelo menos 2300 dólares na região. Na Europa o valor pode chegar aos 45000 dólares. Lá, os Talibans realizam uma atividade semelhante às FARC, onde protegem os agricultores em troca de uma taxa que ajuda a financiar a sua atividade (Business Insider, 2017). A vasta maioria de lucro das substâncias ilegais como a heroína e a cocaína acaba por reverter para grupos terroristas ou organizados.

O sociólogo Robert Merton descreveu os indivíduos que recorrem ao crime como "inovadores", porque trata-se de de uma adaptação dos mesmos a uma sociedade competitiva e materialista, onde muitos têm dificuldades em alcançar riqueza e bens materiais, o que abre as portas ao comportamento criminal de forma a obter maiores posses, e essa tentativa torna-os inovadores (Merton 1938 cit In Decary-Hetu, Aldridge, 2014). A inovação criminal pode ser encontrada em vários tipos de crime, todavia é na internet que têm surgido cada vez mais esquemas criminais. Por exemplo o roubo de cartões de crédito, tal como a utilização de tecnologias de comunicação através da internet para publicitar a venda dos mesmos, ou fornecer os meios necessários para a clonagem dos mesmos, entre outros crimes de diversas tipologias (Decary-Hetu, Aldridge, 2014). Não aplicando-se concretamente a Portugal, muitos locais onde a prostituição é ilegal, a internet serve de intermédio entre ambas as partes. Porém o melhor exemplo de inovação criminal na internet deve ser atribuído à pirataria, nomeadamente ao Napster e ao The Pirate Bay, que tal como o Silk Road, não apresentaram apenas uma inovação, mas sim uma mudança drástica no paradigma da inovação criminal (Decary-Hetu, Aldridge, 2014). Estes serviços permitem aos seus utilizadores obterem e partilharem em musica em formato digital de forma gratuita, e mesmo que o fenómeno da pirataria já fosse uma realidade anteriormente

sob outros meios, com o surgimento destes serviços o crescimento foi colossal, o que obrigou às editoras alterarem os seus métodos de distribuição, adaptando-se a uma nova realidade digital (Decary-Hetu, Aldridge, 2014). Estes fenómenos, mesmo não sendo recentes, demonstram a inovação e alteração de onde decorre o delito, do mundo físico para o virtual (Decary-Hetu, Aldridge, 2014).

O fundador do Silk Road, Ross Ulbricht (sob a alcunha de Dread Pirate Roberts), escreveu nos antigos fóruns do site, agora indisponíveis, que tinha como intenção ajudar os pequenos dealers não violentos e retirar poder aos cartéis violentos (Wired 2014). Na opinião de David Décary-Hétu e Judith Aldridge (2014) esta nova geração de vendedores online apresenta uma mudança drástica no paradigma do tráfico. Mesmo que os lucros entre o Silk Road e o tráfico convencional sejam incomparáveis, este website apresenta um potencial futuro e influência sobre a forma como o mercado das drogas funciona, com algumas características que permitem diminuir a violência. A internacionalização dos criptomercados também é um fator a ter em conta, onde os utilizadores têm maior variedade de compra e de preços, porém os autores afirmam ser precisos mais estudos para averiguar se a preferência dos utilizadores será de vendedores locais ou internacionais (Decary-Hetu, Aldridge, 2014).

Decary-Hetu e Aldridge (2014) afirmam que existe uma perceção errada sobre o Silk Road, defendida por outros autores, onde a maioria das listagens apresentadas são de quantidades relativamente pequenas direcionadas para o consumidor comum (Christin 2012) e a de que os vendedores são os importadores gerais ou os próprios cultivadores, cortando o intermediário (Martin, 2013). Porém, Martin reconhece que nem sempre é possível cortar o intermediário nestes criptomercados (Nasseri, 2014). Na realidade, chegaram à conclusão que a maioria dos compradores era composta por dealers comuns que procuravam aumentar o seu stock (Decary-Hetu, Aldridge, 2014).

De acordo com os mesmos autores, a terminologia utilizada, os preços praticados e as quantidades eram evidências de que o produto para venda fosse com o propósito de revenda. Também destacaram a existência de muitos utilizadores que procuram ou oferecem o ensino de cultivo ou sintetização de uma droga, ou os recursos necessários para tal, o que demonstra que o website é utilizado não só como ferramenta de transações, como também de ensino e de auto produtividade dentro do campo das drogas (Decary-Hetu, Aldridge, 2014).

Para chegar a esta conclusão, os autores criaram um webcrawler, que permitiu coletar cerca de 11853 páginas de anúncios de venda de substâncias ilícitas ativos no Silk Road, coletados entre 13 a 15 de Setembro de 2013, resultando em 1084 vendedores. Este método permitiu aos criminólogos averiguarem em detalhe como funcionava o Silk Road e analisar transferências e determinar os valores incluídos, o que os autores consideram que é um melhor meio de pesquisa comparado ao típico auto-relato, muito utilizado pela criminologia (Decary-Hetu, Aldridge, 2014).

Na altura do estudo, o Silk Road possuía 6 categorias de drogas, medicamentos sujeitos a receita médica (ou "prescriptions", 3953 anúncios ativos), cannabis (2661 anúncios ativos), psicadélicos (1539 anúncios ativos), estimulantes (1274 anúncios ativos), ecstasy (1059 anúncios ativos) e opióides (262 anúncios ativos) (Decary-Hetu, Aldridge, 2014).

O Silk Road teve um "curto" espaço de vida, foi fundado em Fevereiro de 2011 e foi encerrado pela primeira vez pelas autoridades em Junho de 2013 (Norry, 2017). O fundador deste website foi Ross Ulbricht (sobre o nickname de Dread Pirate Roberts), um engenheiro natural do Texas com perspetivas libertárias, que questionava a legitimidade e efetividade da guerra contra as drogas, fundou este website, cujo intuito de transformar o mundo num sítio melhor, com um mercado

livre e fora do alcance governamental. O nome do website foi influenciado pela rede histórica que ligava a Europa à Asia (Norry, 2017).

Com a detenção de Ross Ulbricht e encerramento do Silk Road, o mesmo foi condenado a prisão perpétua. Porém, algum tempo após a sua detenção, surgiu o Silk Road 2.0, gerido por antigos administradores do website anterior. Este renascimento durou apenas 1 ano, pois as autoridades voltaram a ser capazes de rastrear o mesmo, deter os responsáveis e encerrá-lo (Norry, 2017). Posteriormente e ocasionalmente surgem alguns websites sob o mesmo nome, que afirmam ser parte do original Silk Road, todavia, não passam ou de meras imitações ou de tentativas de extorsão (Norry, 2017).

Porém a realidade dos criptomercados já era existente antes do surgimento do Silk Road e não desapareceu após o seu fim. Existiram outros mercados, como o Black Market Reloaded, o Atlantis, o Agora, o AlphaBay, entre outros, sendo que estes obtiveram um grande nível de destaque no universo do tráfico de drogas online, todavia acabaram todos encerrados pelas autoridades (Afilipoaie, Shortis, 2018). Todavia nem todos os criptomercados funcionaram como prometido. Por exemplo, o Sheep Marketplace (Liao et alii, 2016) e o Evolution (Woolf, 2015) terminaram da pior forma para os seus utilizadores. O primeiro, Sheep Marketplace, um utilizador aproveitou-se de uma vulnerabilidade no website para roubar um valor avultado de bitcoins (Liao et alii, 2016), enquanto que o segundo, o Evolution, após um período em atividade, revelou-se ser um "exit scam", com todos os fundos dos utilizadores do website serem roubados por ambos os fundadores (Woolf, 2015). Estes "exit scams" são um fenómeno recorrente nestes criptomercados (ex: Nucleus, outra grande superfície de venda), no qual o utilizador não tem nenhuma forma recuperar os seus fundos ou realizar uma reclamação (National Drug & Alcohol Research Centre, 2016).

Todavia alguns mercados conseguem sobreviver a todas as adversidades. O Dream Market é um destes casos, foi fundado em 2013 e é dos muito poucos websites com um nome conotado que conseguiu resistir aos esforços das autoridades, com quase cerca de 5 anos de existência (National Drug & Alcohol Research Centre, 2016). Por curiosidade, outros não duram muito tempo. Em 2014, as autoridades holandesas encerraram um criptomercado pelo nome de Utopia 8 dias depois de entrar online (BBC, 2014).

Podemos constatar que estes websites por norma após surgirem, passado um determinado tempo desaparecem, onde no seu lugar surgem outros mercados com novos métodos mais eficazes. Porém, o criptomercado atual com maior potencial não se trata de um website, mas sim de uma aplicação para o computador. Trata-se do OpenBazaar, um programa que encontra-se em constante desenvolvimento e que traz para este universo "novas regras" e garantias (Fox-Brewster, 2016). A melhor forma de descrever o OpenBazaar é descreve-lo como um vasto mercado, contendo pequenos negócios locais e indivíduos que têm algo em segunda mão por exemplo para vender, ou qualquer outra pessoa ou entidade que pretenda vender ou comprar algo. Isto também atraí anúncios de produtos de caráter legal duvidoso. Esta aplicação funciona através da utilização de um programa de computador que utiliza a mesma tecnologia da bitcoin, a blockchain, permite a intermediação e o contacto entre ambas as partes (via P2P) de forma confidencial (desde que ambas as partes mascarem os seus IP's) (Fox-Brewster, 2016). Mas as inovações deste serviço não passam apenas pela mudança de websites para ficheiros executáveis. O OpenBazaar por exemplo, em contraste do que era aplicado por todos os criptomercados da web não retira uma percentagem das transações efetuadas, criando um mercado totalmente descentralizado. (Fox-Brewster, 2016).

Existe uma grande potencialidade que os criptomercados transformem-se neste tipo de serviço totalmente descentralizado no futuro, o que complicará a possibilidade das autoridades realizarem as suas operações (Décary-Hétu, Giommoni, 2017).

Nos estados americanos onde o consumo recreativo ou medicinal da marijuana é legal, é possível obter uma aplicação para o telemóvel denominada de "High There", que pretende servir de uma aplicação de encontros ou namoros, tal como o *tinder*, porém, tem por objetivo ligar pessoas cujo interesse mútuo é o consumo de marijuana (Godoy, 2015). No Brasil é utilizada uma aplicação denominada de "Who Is Happy", que identifica no mapa outros utilizadores que usem marijuana e utilizem a mesma plataforma (Godoy, 2015).

Mas no geral, podemos concluir que a utilização de criptomercados e destas aplicações legais para compra e venda de drogas, mesmo que apresentem fatores positivos, é essencial realizar mais estudos sobre as mesmas, ou até regulamentar os mesmos.

1.5 Os desafios das autoridades e a prevenção do fenómeno

Como já foi referido diversas vezes durante este projeto, as autoridades e governos enfrentam um sério desafio, cada vez mais preocupante (Barratt et alii, 2013, cit in Nasseri 2014). A confidencialidade das moedas virtuais e das ferramentas encriptadas revelam-se num desafio complicado para as autoridades (Martin, 2013).

Para Martin (2013), é importante ter uma perceção na orientação da perspetiva cibercriminal e não a de tráfico tradicional, visto que este mercado é impulsionado através de tecnologias computacionais, em particular, através da Internet, porém, sem ignorar o facto de que os utilizadores destes mercados continuam a violar o mesmo bem jurídico que o tráfico tradicional quebra (Cit in Nasseri, 2014). Martin (2014) e Christin (2012), salientam a importância de não interpretar os criptomercados apenas como um fenómeno restrito às drogas, visto que estes websites fornecem também

outro tipo de atividades, criminais ou não. É crucial o seu estudo e compreensão pelas autoridades (Cit in Nasseri, 2014).

O facto destas redes encontrarem-se num espaço encriptado, onde as suas transações são realizadas através de criptocurrencias, complica os trabalhos das autoridades para combater este fenómeno, sendo que esses esforços demonstram ter um impacto muito reduzido na tentativa de diminuir a rapidez da expansão destes serviços (Nasseri, 2014).

De acordo com Van Hout e Bingham (2013), a confidencialidade dos criptomercados e das criptomoedas oferecem sérias dificuldades para as autoridades, mas Barratt (2012) menciona que existem métodos para as autoridades conseguirem contornar estas adversidades, que passam maioritariamente pelo controlo postal, visto que a encomenda para ser entregue tem que passar pelos correios, e caso intercetadas facilitam o reconhecimento de ambos os lados da transação e permitem a interferência das autoridades (cit in Nasseri 2014).

Porém, Van Hout e Bingham (2013), Basu (2014), Martin (2013) e Christin (2012), reconhecem a dificuldade em garantir a eficácia destas políticas de controlo postais. O argumento dado por Martin (2013) realça a rápida globalização que por sua vez resultou num maior volume de encomendas, o que leva a que as percentagens de encomendas intercetadas sejam menores, pois como o autor afirma "acaba por ser como encontrar uma agulha num palheiro". Jenner (2011), por sua vez, afirmou que é impossível para as autoridades determinarem os números reais de encomendas que entram pelas fronteiras de uma nação (cit in Nasseri, 2014).

Para Nasseri (2014), as autoridades utilizam os mesmos meios para tentar quebrar os mercados de droga tradicionais e os criptomercados. Estes métodos passam por interferir com a rede, interferir com a sua infraestrutura financeira, interferir com o seu processo de entrega ou realizar operações encobertas.

O primeiro meio descrito por Nasseri (2014) passa pela interferência com a rede. Visto que o Tor é um elemento fulcral para o funcionamento dos criptomercados, é natural que as autoridades tentem interferir com o mesmo. Todavia os criptomercados representam uma fração muito pequena do tráfego que passa pela rede Tor, e atacar a rede no geral seria injusto para aqueles que a utilizam com um intuito legal. Porém, o Tor tem algumas vulnerabilidades que podem ser exploradas sem terminar a rede na totalidade. Todavia, adaptar as autoridades e treina-las a localizar estes serviços no Tor sairia muito dispendioso e acabaria por não se revelar eficaz caso o utilizador soubesse mascarar os seus passos, como por exemplo utilizar um VPN (Nasseri, 2014).

O segundo ponto descrito refere a interferência com a estrutura financeira. Visto que as transações estão dependentes das moedas virtuais altamente voláteis, as autoridades são capazes de tentar criar manipulações no valor da moeda, diminuindo o valor da mesma de forma a atrasar transações. Porém, graças à cada vez maior oferta de criptomoedas, esta tática parece ser ineficiente para combater este fenómeno (Nasseri, 2014).

O terceiro ponto enquadra-se na tentativa de interferência com o processo de entrega. Já foi referido que vários autores são apologistas de um maior controlo alfandegário e fronteiriço, porém os vendedores nas descrições dos seus produtos não parecem preocupados com este controlo, acrescentando o facto de realizarem entregas internacionais. Os compradores são alertados a evitar encomendar de vendedores cujo

país de origem da encomenda tem uma certa conotação com a exportação de drogas, como o caso da Colômbia, de forma a evitar atrair atenções por parte das autoridades. Não obstante, os próprios vendedores utilizam técnicas sofisticadas de dissimulação das substâncias de forma a contornar as autoridades, que requeria uma busca intensiva para as detetar. Este cenário exige uma grande quantidade de tempo e mão de obra disponível, sem mencionar os custos envolventes (Nasseri, 2014).

O quarto ponto refere as operações encobertas, que até o momento revelam ser a estratégia mais eficaz e bem sucedida de atacar este fenómeno. Barratt et alii (2014) afirmam que as autoridades deveriam aplicar métodos tradicionais de policiamento, onde o polícia assume o papel encoberto de comprador ou vendedor de droga, de forma a obter mais provas relacionadas com os envolvidos nestes mercados. Porém, para além de dispendiosas e exigirem largas quantidades de tempo para obter provas suficientes, esta tática parece não conseguir ser capaz de dissuadir os atores criminais de voltarem a cometer o ato, tal como não parece ser eficaz em evitar o surgimento de novos mercados deste género (Nasseri, 2014).

Estes são os quatro pontos que de acordo com Nasseri são implementados pelas autoridades. Todavia o mesmo autor sugere uma nova abordagem, o Laissez-faire, ou simplesmente, não fazer nada. O autor admite que esta opção possa parecer controversa, todavia, tendo em conta as largas quantias monetárias que são investidas no combate às drogas e que estes serviços promovem a redução de danos e a não-violência, deitar abaixo estes sistemas poderia acarretar sérias consequências (Nasseri, 2014).

Torna-se evidente que as autoridades têm pouco sucesso em combater este fenómeno, acrescendo-se o facto de terem custos elevados e de ser necessário investir muito tempo, como também não existem garantias de que os membros afetados não optem

por utilizar outros criptomercados ou que esses mesmos mercados não voltem a emergir sobre nomes ou responsáveis diferentes (Nasseri, 2014). De acordo com Benson (2014), quando um mercado é encerrado, os seus utilizadores tendem a mudar-se para outros de forma a poder dar continuidade ao seu ofício (Nasseri, 2014).

Atualmente, os criptomercados não têm grandes efeitos sobre o trafico convencional, ou pelo menos em reduzir este fenómeno, todavia, com o seu rápido crescimento, existe o potencial deste fazer danos ao longo prazo, logo, os governos e autoridades deveriam adaptar-se e preparar-se para combater esta nova realidade (Nasseri, 2014).

Para alguns autores como Christin (2012), Martin (2013) e Van Hout e Bingham (2013), as autoridades não deveriam intervir de momento nestes mercados, argumentando o seu potencial na redução da violência e nas suas políticas de redução de danos.

As autoridades obviamente têm todo o interesse em terminar com a atividades destas redes, todavia a sua incapacidade para as terminar é notória. As políticas utilizadas para terminar com os criptomercados, para além de muito complicada, é bastante dispendiosa e difícil de implementar (Martin, 2013). Nasseri (2014) defende que antes das autoridades intervirem, estas devem ter em consideração todos os aspetos positivos e negativos destes mercados.

Em contraste ao que é visível na tradicional guerra contra as drogas tradicional global, e apresentado em vários estudos empíricos (Martin, 2013; Van Hout, Bingham, 2013; Christin, 2012) os criptomercados apresentam uma mudança drástica na redução da violência adjacente ao tráfico de droga, nomeadamente por eliminar a necessidade de encontros diretos entre as partes.

Mesmo que as autoridades sejam capazes de eficazmente combater este fenómeno, Martin (2013) realça que isso não impedirá dos utilizadores recorrerem ao mercado tradicional, com maiores perigos (Cit in Nasseri, 2014).

Quanto ao fator da redução de danos, os estudos relacionando ambos os campos tem vindo a aumentar. Enquanto que as fontes principais de programas educacionais e dissuasoras do consumo de substâncias derivem de programas governamentais ou educacionais (Moore, 2008; cit in Nasseri, 2014), a existência de fóruns públicos nos criptomercados facilita a comunicação entre os usuários, onde partilham instruções seguras e educam-se uns aos outros para os riscos da utilização de drogas, tal como possibilita a partilha de histórias anonimamente, o que facilita e encoraja a participação. Isto possibilita aos usuários que participem nestas discussões que possam saber como evitar uma experiência desagradável com estas substâncias (Barratt, 2012; Cit in Nasseri, 2014). De acordo com um estudo realizado por Barratt et alii (2013), a larga maioria dos inquiridos revelou que frequentam os referidos fóruns com o intuito de obter mais experiência no tema e de reduzir os danos (Barratt et alii, 2013; Cit in Nasseri, 2014).

Para Barratt (2012), os criptomercados deveriam ser enquadrados na perspetiva da saúde, visto que promovem políticas de redução de danos, fornecendo aos usuários informação mais relevante e compreensiva, através da comunicação e partilha de informações e experiências (Cit In Nasseri, 2014).

Em termos de grandes operações feitas contra os criptomercados, destacam-se principalmente a Operação Onymous, a Operação Bayonet e a Operação GraveSac, onde é notória uma existência de cooperação entre entidades governamentais para o combate aos criptomercados (Décary-Hétu, Giommoni, 2017; Afilipoaie, Shortis, 2018).

A Operação Onymous foi levada a cabo em 2014 por um conjunto de autoridades, como a Europol, o FBI, a ICE, a HIS e a Eurojust, e tinha por objetivo terminar as

vendas e distribuições de drogas, que eram vendidos nestes criptomercados. (Europol, 2014). Como resultado desta operação, 410 serviços foram encerrados, foram feitas 17 detenções, tal como foram apreendidas bitcoins, dinheiro, substâncias ilegais, entre outros materiais (Europol, 2014). Alguns destes serviços que foram terminados destacam-se a o Silk Road 2, o Cloud Nine e o Hydra, e aqueles que conseguiram sobreviver, como o Agora e o Evolution, sofreram algumas consequências desta operação, tal como sofreram redução no número de vendas e no registo de novos utilizadores, que todavia, após uns meses regressou à normalidade (Décary-Hétu, Giommoni, 2017).

Esta operação revela que afinal as autoridades possuem meios capazes de afetar os criptomercados, como também sugere que afinal de contas a confidencialidade não é totalmente garantida (Décary-Hétu, Giommoni, 2017).

Previamente, outros autores mencionaram que o encerramento do Silk Road original pouco ou nenhum impacto teve sobre os criptomercados, e que não deteve os participantes de continuarem com estas atividades, onde se destacou a migração destes para outros mercados. Porém, após a Operação Onymous através de um estudo, Décary-Hétu e Giommoni (2017) aperceberam-se que esta operação teve de facto um impacto sobre os criptomercados.

Quanto ao preço das drogas, não existem evidencias que demonstrem que o mesmo aumentou, onde na realidade aparenta ter existido uma ligeira queda no preço, que pode ser associada à volatilidade da bitcoin (Décary-Hétu, Giommoni, 2017). Visto que após uma operação desta escala onde várias moedas bitcoin são confiscadas pelas autoridades, possivelmente houve um grande numero de pessoas que vendeu as suas bitcoins, o que pode justificar esta queda repentina no preço.

Após esta operação conjunta, os websites sobreviventes como o Agora e o Evolution sofreram uma queda no número de vendedores ativos, que posteriormente veio a normalizar e a voltar à tendência de crescimento rápido. Isto pode-se justificar com o

facto dos "dealers" quererem evitar chamar a atenção das autoridades após uma operação em larga escala e tirarem um pequeno período para deixar afastar a atenção policial (Décary-Hétu, Giommoni, 2017).

A operação também aparenta ter afetado o comportamento dos indivíduos que vendiam nestes websites que foram encerrados, muitos destes optaram por não enveredar por outros criptomercados, enquanto que os que já operavam nos mercados "sobreviventes" continuaram em atividade. É possível que de facto os valores de vendedores que passaram a sua atividade para outros websites indicados no estudo de Décary-Hétu e Giommoni sejam maiores, visto que podem ter optado por um nome de utilizador diferente do anterior ou que apenas registaram a conta após a realização do seu estudo (Décary-Hétu, Giommoni, 2017). Os mesmos autores argumentam a possibilidade de após esta operação, pode ter existido uma percentagem de vendedores que optaram manter-se em negócio apenas no mercado tradicional de droga (Décary-Hétu, Giommoni, 2017).

O estudo indica que o numero de anúncios ativos diminuí ligeiramente, mantendo-se minimamente estável, sugerindo que a operação conjunta não conseguiu afetar o fornecimento e disponibilidade de substâncias por via online, visto que a quantidade de anúncios existentes na altura eram bem capazes de satisfazer toda a demanda de potenciais clientes (Décary-Hétu, Giommoni, 2017).

Graças à operação, os autores notaram num decréscimo das vendas nos websites que resistiram a esta fiscalização. Porém, foi apenas uma questão de tempo, visto que semanas depois da operação, os números de acabaram por ser ainda maiores aos anteriores à Operação Onymous (Décary-Hétu, Giommoni, 2017).

Outros estudos (Brixton, Bingham, 2015; Van Buskirk et alii, 2014) sugeriam que estas operações policiais poderiam vir a ser positivas para os criptomercados, pois de uma certa forma funcionavam como "publicidade gratuita" e davam a conhecer ao público geral a existência destes serviços. Todavia, no estudo de Decary-Hétu e

Giommoni (2017) isto não é aparente, dado que o aparecimento de novos "dealers" foi menor, ao invés do numero de consumidores, que nos meses posteriores aumentou (Décary-Hétu, Giommoni, 2017).

O estudo conclui que a Operação Onymous afetou os utilizadores dos criptomercados, porém, apenas por um breve período de tempo (Décary-Hétu, Giommoni, 2017). A oferta e demanda foi claramente afetada, que, todavia, o preço dos produtos manteve-se na mesma ordem, onde o impacto conseguiu também alcançar outros websites que não foram alvo da operação (Décary-Hétu, Giommoni, 2017). Os resultados sugerem que os encerramentos pelas autoridades não parecem possuir efeitos em conseguir eficazmente diminuir o número de vendas nos criptomercados, como também em conseguir dissuadir alguns utilizadores de cessarem a utilização destes serviços. Os autores afirmam que estes métodos são uma forma ineficaz de combater este fenómeno, mas que todavia, consegue desestabilizar e até terminar a sua atividade (Décary-Hétu, Giommoni, 2017).

Porém em 2017 houve uma grande mudança na metodologia das operações das autoridades. Entre Junho e Julho desse mesmo ano, através de uma operação conjunta entre as autoridades americanas e autoridades europeias, como também com apoio de outras instituições públicas e privadas, foram deitados abaixo dois grandes criptomercados, o Hansa e o AlphaBay. Dessa operação, foram apreendidos milhões de dólares, tal como foram efetuadas diversas detenções (Afilipoaie, Shortis, 2018).

Essa grande operação conjunta consistia em duas "pequenas operações". A Operação Bayonet, desempenhada na maioria pelas autoridades americanas com vista o AlphaBay e a Operação GraveSec, feita na maioria por autoridades europeias com vista o mercado Hansa. Esta provou ser uma grande mudança nas estratégias e táticas utilizadas pelas autoridades, revelando-se muito mais eficaz no combate a este fenómeno (Afilipoaie, Shortis, 2018).

A operação começou de forma minimamente inédita. A 20 de Junho de 2017, a unidade de combate ao cibercrime holandesa (NHTCU) infiltrou-se no mercado Hansa e tomou conta das suas operações, todavia, ao contrário do que seria expectável, não o encerrou. Entretanto foram detidos pelas autoridades alemãs dois dos administradores do website, que revelaram mais informações sobre as operações. As autoridades aproveitaram para obter e investigar o código fonte do website, de forma a poder estuda-lo e procurar vulnerabilidades, como também com o intuito de melhorar a capacidade de recolha de informações destes serviços (Afilipoaie, Shortis, 2018). Destaca-se aqui outro fator crucial para a concretização desta operação, que foi a colaboração de uma entidade privada para concretizar a infiltração, neste caso, da empresa de cibersegurança BitDefender (Afilipoaie, Shortis, 2018).

A operação Bayonet começou no dia 5 de Julho, e conseguiu encerrar o AlphaBay (na altura um dos maiores criptomercados) e deter o seu fundador, um jovem de 25 anos canadense, Alexandre Cazes. Como consequência do encerramento deste serviço, o numero de inscrições no Hansa aumentou drasticamente, o que levou às autoridades holandesas, visto que na altura eram estas que detinham o controlo do website, a fechar a possibilidade registo no website. Esta opção foi tomada derivado ao facto de tornar-se mais difícil de analisar toda a informação com um número tão grande de utilizadores, mas que todavia, mesmo sem terem noção que a administração do website fora comprometida, os utilizadores aplaudiram, porque assim era possível manter o fluxo normal do website, aumentando a confiança depositada nos administradores que na realidade eram as autoridades (Afilipoaie, Shortis, 2018).

Apenas 27 dias depois da NHTCU se infiltrar no mercado Hansa é que o FBI e a Europol emitiram um comunicado conjunto que procederam ao encerramento destes serviços. Nos seus resultados, a NHTCU monitorizou uma média de 1000 transações diárias, como também angariou cerca de 10000 moradas e várias mensagens privadas de membros do mercado Hansa. Por sua vez, o FBI estimou que obteve a identidade de cerca 200000 utilizadores e cerca de 40000 vendedores do AlphaBay (Afilipoaie, Shortis, 2018).

Afilipoaie e Shortis (2018) apontam para uma combinação de diversas táticas operacionais, o honeypot (no caso da operação GraveSec), a exploração da infraestrutura tecnológica, a gestão da migração, a perca de confiança e as lições estratégicas.

A utilização de um honeypot por exemplo foi uma grande inovação nos métodos para obter informações sobre estes mercados, onde foram não só capazes de obter informações, como também de administrar o mesmo. Tratou-se de uma operação coordenada e ponderada, que demonstrou um grau de compreensão do funcionamento destes serviços, como também uma compreensão tecnológica (Afilipoaie, Shortis, 2018).

Vários mecanismos de segurança destes websites foram também explorados pelas autoridades, como por exemplo as credenciais de login. É comum estes websites removerem automaticamente os metadados das imagens colocadas pelos utilizadores, mas as autoridades usaram isto a seu favor, desativando essa funcionalidade que lhes permitiu aceder aos mesmos, o que lhes fornecia informações geográficas de onde a foto foi tirada. As autoridades exploraram também o sistema de mensagens encriptadas do website e obter o seu conteúdo. Também modificaram um ficheiro de texto para excel, que forçava o computador do utilizador a fazer um ping aos servidores das autoridades, sendo possível detetar o IP de origem, porém, caso o usuário não estivesse a mascarar o seu IP com um VPN ou o Tor (Afilipoaie, Shortis, 2018).

Seguindo a tendência de quando um criptomercado é encerrado, muitos utilizadores migram para outros serviços. Nestas operações, as autoridades revelaram-se prontas para gerir a eventual migração, o que lhes permitiu maximizar as informações adquiridas (Afilipoaie, Shortis, 2018).

As autoridades também tentaram afetar a confiança que os utilizadores têm a estes serviços (Afilipoaie, Shortis, 2018). O FBI atrasou a declaração da operação contra o

AlphaBay de forma a criar a ideia pelos utilizadores que tinha ocorrido um "exit scam" (o administrador fugir com todos os fundos), de forma a criar algum pânico entre os utilizadores, tal como quando os utilizadores descobriram que as autoridades europeias tinham controlo sobre o mercado Hansa e sob todo o seu conteúdo, ficaram obviamente apreensivos e receosos. As autoridades holandesas e americanas deslocaram-se até os domicílios dos seus respetivos utilizadores nacionais, alertando-os para se afastarem dos criptomercados e criando um certo medo nos mesmos, pois agora ficam com a ideia de que estão sendo monitorizados (Afilipoaie, Shortis, 2018).

Afilipoaie e Shortis (2018) destacam esta mudança no paradigma da metodologia das autoridades perante os criptomercados, realçando a cooperação internacional entre as autoridades e vários sectores públicos e privados, demonstrando um maior conhecimento e experiência sobre este campo que outrora, implementando outras táticas como a quebra de confiança, que é algo fulcral para o bom funcionamento de um mercado deste género. Ao adiar o encerramento do serviço e danificar mais a confiança dos utilizadores, os autores creem que as autoridades foram capazes de infligir mais dano à comunidade. Porém, reconhecem que esta perceção vai contra a potencialidade da utilização de criptomercados para a redução de danos (Afilipoaie, Shortis, 2018).

Assim, Afilipoaie e Shortis (2018) concluem que estas operações serviram para as autoridades ganharem maior compreensão sob o ambiente dos criptomercados como também demonstram uma evolução e métodos mais eficazes de afetar as mesmas. Pode ser argumentado também que estas ações não foram capazes de erradicar por completo o fenómeno, porém foram capazes de quebrar a confiança em alguns utilizadores. Todavia, essa falta de confiança pode gerar o surgimento de um novo paradigma de criptomercado descentralizado, como o OpenBazaar, que criará novos problemas para as autoridades (Afilipoaie, Shortis, 2018).

Capítulo II- Contribuição Empírica

Neste capítulo será apresentado uma proposta de inquérito direcionada aos utilizadores destas redes. Será descrito o método a utilizar e os seus participantes, o material e os procedimentos necessários para a realização da mesma e por último os resultados esperados.

2.1. Método

Em primeiro lugar é necessário ter em conta o campo e ambiente onde se enquadram estes criptomercados. O objetivo dos mesmos é de garantir a confidencialidade dos utilizadores, logo a realização dos típicos inquéritos de rua não teria sucesso por diversas razões, a primeira sendo obviamente o desejo de manter esse anonimato, tal como a possibilidade de encontrar um público de amostra muito reduzido ou até nulo, visto que este mercado é relativamente pequeno e a sua utilização em território nacional aparenta ser limitada. Até mesmo a realização de inquéritos online pode ser recebida com desconfiança por parte dos utilizadores, visto que pode tratar-se de uma tática policial para rastrear a origem do IP e eventualmente punir ou advertir o utilizador.

Logo o melhor meio para obter as respostas é no próprio meio onde os utilizadores se deslocam para obter o seu produto, ou seja, na internet. Os criptomercados provavelmente não são a favor da realização destes inquéritos e os seus utilizadores também não devem apreciar a ideia deste serviço permitir a utilização do mesmo por terceiros, mesmo que seja para fins académicos.

Desta forma, assume-se que o melhor meio para realizar este inquérito seria num fórum cujo tema de discussão principal fossem estes criptomercados, onde este serviço não poderia recolher absolutamente mais nenhum detalhe sobre o inquirido

exceto as suas respostas. Os utilizadores devem sentir-se confiantes em responder, tal como é imperativo que não se sintam observados por outra entidade. Todas as perguntas devem ter um caráter de não obrigatoriedade de resposta, de forma a que caso um utilizador não se sinta confortável em responder a uma questão este possa passar para a seguinte, assim, obtendo assim informação de qualquer das formas nos outros campos. Isto pode apresentar uma ameaça para as médias finais do inquérito, visto que em algumas perguntas todos os inquiridos tenham respondido enquanto que noutras o valor foi mais reduzido. Todavia, neste inquérito é fulcral o anonimato e dar a hipótese de escolha de responder ou não responder ao inquirido.

2.1.1. Participantes, Objetivos e Questões de Investigação

Os participantes deste inquérito são naturalmente os utilizadores destes criptomercados, quer sejam os consumidores que apenas compram as substâncias, quer sejam os vendedores que os fornecem, ou aqueles que se enquadrem em ambas as categorias, ou quer sejam assíduos ou que apenas tenham utilizarado este serviço uma vez.

Com este inquérito pretende-se obter mais informação geral sobre estes mercados, quem os utiliza e porque que o fazem. Mais concretamente, tratam-se de questões como por exemplo o tipo de droga adquirida e a satisfação do produto, quantos criptomercados utiliza ou se apenas limita a um e quantas vezes efetuou uma encomenda, tal como se alguma vez já teve uma encomenda apreendida ou algum problema com as autoridades. Pretende-se também dar a possibilidade de facultar uma resposta aberta, visto que as hipóteses de escolha múltipla possam ser limitadas e não correspondentes com a realidade desse utilizador.

As questões principais centrar-se-ão na temática da droga adquirida, podendo extender-se a outras questões como a quantidade encomendada e a avaliação da mesma. Porém, questões como a preferência dos utilizadores, os porquês da utilização destes serviços, a sua satisfação com os mesmos, tal como problemas com as autoridades. Outra pergunta que deveria ser feita devido à escassez de estudos sobre a mesma, é a localização geográfica do utilizador, porém, esta questão contradiz ligeiramente a garantia de confidencialidade, logo, de forma a evitar uma resposta errónea do utilizador, todas as questões devem ser de caráter de resposta opcional.

2.1.2. Material e Procedimentos

Em primeiro lugar, é necessário encontrar um fórum ou website relacionado com estes criptomercados, diretamente ou indiretamente, e pedir autorização para realizarem o inquérito. Esta tarefa pode ser muito complicada por diversos motivos, em particular o facto destes websites não cederem a estes ou a outros quaisquer tipos de pedido que envolvam o estudo dos seus utilizadores ou ao facto de poder criar uma certa desconfiança dos seus utilizadores para com a administração, logo é complicado obter o apoio de um destes serviços para realizar o inquérito.

Na eventualidade de não ser possível encontrar nenhum serviço que facilite a realização destes inquéritos, o mesmo terá que ser realizado por vias mais tradicionais, como os inquéritos utilizando o Google Forms, o que resultará em menor confiança por parte dos utilizadores e receio em realizar o inquérito, logo a amostra será menor.

Caso o primeiro parâmetro seja cumprido, será necessário implementar no website (de forma a não recorrer a serviços terceiros que possam manter os dados para si mesmos) um serviço de inquéritos, confidencial. É fulcral que as perguntas deste sejam de

caráter opcional, de forma a não interferir com o estudo, como mencionado anteriormente. Questões que se incidem sobre questões pessoais devem ser evitadas ao máximo, como por exemplo pedir o nome, o seu emprego ou a sua cidade. Todavia, algumas questões de teor pessoal podem e devem ser realizadas, pois o seu conteúdo pode ser extremamente interessante para futuros estudos, questões como a idade do utilizador, de forma a obter uma média de idades e ter uma noção de qual a faixa etária que mais recorre a estes serviços. Outra questão de teor pessoal, mas com grande interesse académico seria o país do utilizador. Visto que a larga maioria das encomendas enviadas não são intercetadas na alfandega, é complicado determinar quais são os principais "importadores e exportadores" deste serviço, além do facto de que as encomendas apreendidas nas alfandegas podem ter sido adquiridas por outros meios mais convencionais. Todavia, esta pergunta tem um certo teor pessoal que o utilizador talvez não se sinta confortável em responder. Logo, questionar qual a sua cidade está completamente fora de questão, deixando apenas a possibilidade do utilizador responder qual a sua nacionalidade se assim o entender.

O inquérito deverá permanecer online durante um tempo estipulado, onde dado o fim deste, os resultados devem ser exportados e inseridos num programa que facilite o investigador a retirar conclusões e resultados, como por exemplo o SPSS. Algumas, possíveis, questões para este inquérito encontram-se no Anexo 1 deste projeto.

2.2. Resultados Esperados

Visto que este trabalho trata-se de um projeto de graduação e dada as complicações para a realização deste estudo, o mesmo não foi efetuado, contudo sendo apresentado aqui apenas como uma simples sugestão de um inquérito a ser realizado. Todavia, algumas respostas já nos são dadas por alguns dos autores referidos neste projeto. Podendo estar corretas ou não, sempre servem de ponto de partida para uma melhor

noção e compreensão destes mercados. O questionário pode ser analisado nos Anexos.

Quanto à primeira parte do inquérito, nenhum autor refere a faixa etária dos utilizadores destes mercados. Porém, podemos assumir que uma grande proporção dos mesmos é jovem, dado que é uma geração que se encontra mais "apegada" às tecnologias, como também os toxicodependentes mais velhos, para além de preferirem o método tradicional pois sempre foi a sua realidade, não devem estar tão bem assemelhados com o uso de ferramentas tecnológicas como VPN's ou o Tor, ou até a própria utilização das moedas virtuais. Esta ideia até pode estar errada, pois não possui nenhum estudo que a fundamente, todavia, existe uma grande possibilidade de que o resultado venha a ser esse. Concluindo esta questão, podemos relembrar que o fundador do Silk Road e o do Evolution eram ambos relativamente novos, o que é a favor do argumento dado. Quanto aos países, os dados também são escassos, mas vários autores realçam países como os Estados Unidos da América, o Canadá a Austrália e a Holanda (Barratt (2012), Martin (2014), Décary-Hétu e Aldridge (2014), Broséus et alii (2016), Décary-Hétu e Giommoni (2017), Afilipoaie e Shortis (2018)).

Na segunda parte os resultados são de valores extremamente variáveis. Algumas das questões já nos foram respondidas por alguns autores, como por exemplo se os utilizadores possuem uma conta em mais que um site. Broséus et alii (2016) demonstra que sim, em particular os vendedores, que se encontram espalhados por diversos sites, em alguns casos até vendendo outro tipo de drogas. Porém, as restantes perguntas desta secção ainda não possuem resposta, logo não é possível expectar um resultado.

Quanto à terceira parte do questionário, persiste o problema de escassez de estudos, porém pode dever-se ao facto dos autores focarem-se noutras questões essenciais e

pertinentes sobre os criptomercados do que propriamente nas questões apresentadas nesta parte do inquérito. As estatísticas demonstram que o maior número de anúncios no Silk Road eram de marijuana, por isso é expectável que a substância ilícita com maior número de venda seja este e o menor número sejam os opioídes (Decary-Hetu, Aldridge, 2014) .

A última parte do inquérito sofre do mesmo problema, onde algumas questões colocadas ainda não obtiveram resposta. Porém algumas delas sim, como por exemplo, quanto aos problemas alfandegários, podemos esperar um número baixo, pois de acordo com um estudo de Jenner (2011), as autoridades australianas apenas foram capazes de apreender 20% das encomendas que continham drogas que deram entrada no país (Cit In Nasseri, 2014). Algumas questões são de resposta "quase óbvia", como por exemplo se os utilizadores consideram os criptomercados como um meio mais cómodo e seguro para ambas as partes envolvidas, todavia também ainda não existe bibliografia que discuta estas questões. Quanto à redução de violência, este valor também será quase nulo devido ao contexto cibernético destes mercados e da separação que se faz entre o vendedor e o usuário (Martin, 2014).

Conclusões

O consumo de drogas é um fenómeno que dentro de qualquer contexto imaginável muito provavelmente não cessará. O consumo destas substâncias quase que se encontra enraizado no ser humano, seja por um desejo de fugir à realidade ou devido a motivos de saúde. Tendo em conta que independentemente do seu consumo ser legal ou não, existe uma demanda pelo produto e esta não deve ser ignorada. Isto pois a substância, mesmo sendo ilegal, enquadra-se num mercado, e o mercado possui leis para o seu bom funcionamento, como por exemplo a Lei da Oferta e da Procura, que afirma que quando existe pouca procura e muita oferta por um produto, o seu preço aumenta, e quando a procura é larga e a oferta mínima o seu preço aumenta.

Ora, ao ilegalizar o consumo e a venda de drogas, é óbvio que a oferta diminuirá, todavia, a demanda, ou procura, continua lá, possibilitando a indivíduos que necessitem de algum ofício possam embarcar nesta aventura lucrativa. Contudo esta perspetiva não ajuda a erradicar este fenómeno, pois não ataca o motivo de existir o tráfico de drogas, que é a demanda pelo produto. Isto foi possível constatar-se nos anos 20 durante a infame "Lei Seca" nos Estados Unidos, que terminou com a venda de álcool, colocando milhares no desemprego e abrindo portas ao crime organizado, que detetou um negócio rentável. Porém, estas não erradicaram o problema do alcoolismo, muito pelo contrário, a venda do álcool passou de bebidas mais leves, como a cerveja para bebidas cujo teor alcoólico era muito maior, como o whiskey, de forma a rentabilizar mais o negócio e receber maior capital.

Enquanto existir um grupo de indivíduos que está disposto a pagar por uma droga, existirá sempre alguém que, para cumprir as regras do mercado, esteja disponível para satisfazer essa demanda e a correr o risco da mesma. Logo, os governos têm que se adaptar à ideia de que o consumo é uma realidade difícil de erradicar e focar os gastos

utilizados no combate ao tráfico em políticas e iniciativas dissuasoras do consumo, tal como fornecer um maior apoio estatal a programas de inserção. Desta forma, ao focar-se na raiz do problema, que é o facto de existir uma demanda, o estado poderá ser mais eficaz em terminar com grande parte do controlo criminal sobre este mercado, ou pelo menos torná-lo menos lucrativo e menos tentador ao crime. Existem outras perspetivas mais radicais que defendem por exemplo que todas as drogas deveriam ser legais, outras que defendem a legalidade dos mesmos, mas sob controlo total estatal, o que permitiria ao estado arrecadar algum capital com a taxação que poderia vir a ser investido em campanhas e programas de dissuasão do consumo destas substâncias.

Estes criptomercados representam uma alteração drástica no paradigma do tráfico, ao apresentar-se como um meio menos violento e mais seguro para os seus utilizadores. Estes também podem servir de ponto de partida para a redução de danos, avisando e sensibilizando os usuários para os riscos do consumo, como também de como utiliza-los de forma segura e responsável.

Todavia estes websites não cortam o intermédio. Numa perspetiva ligeiramente utópica, e ignorando todas as legislações em vigor, caso os cultivadores soubessem trabalhar com as novas tecnologias e fossem completamente capazes de realizar os envios por si mesmos, entrava-se num campo onde todos os lucros da substância revertem para aquele que o fez, terminando-se com a injustiça dos lucros reverterem em grande maioria para o intermediário, na maioria das vezes, o crime organizado. Aqui, quem receberia os lucros do trabalho seria um agricultor de classe baixa, que possui poucas posses. Para além deste argumento, é possível argumentar que a pureza do produto seria largamente maior do que a típica pureza "de rua", visto que a utilização de matérias "cortantes" seria nula, visto que esta é feita pelos vários intermediários de forma a aumentar o seu lucro.

Estes criptomercados apresentam grandes potenciais, principalmente pelas suas inovações tecnológicas. É possível argumentar que o futuro do tráfico passe pelo uso destas tecnologias, mas não só. Tudo indica para que estas tecnologias sejam cada vez mais utilizadas e cabe-nos a nós saber utiliza-las de forma responsável, visto que estes mercados podem não só se restringir apenas a drogas. Todavia, não podemos ignorar o facto de que estes serviços podem ser utilizados com intuitos moralmente ou eticamente questionáveis.

Concluindo, realça-se o que foi abordado pela larga maioria dos autores que falaram sobre os criptomercados, que é necessidade de mais estudos sobre este fenómeno de forma a conseguirmos compreende-lo. Se o futuro da sociedade passa pelo uso de criptomercados ou moedas virtuais, convém aprendermos o máximo sobre elas enquanto podemos, de forma a evitar potenciais abusos.

Referências Bibliográficas

Adam, M. (2017). Bitcoins não são legais mas podem ter de pagar impostos. [Em linha] Disponível em <http://www.jornaldenegocios.pt/mercados/detalhe/bitcoins-nao-sao-legais-mas-podem-ter-de-pagar-impostos>. [Consultado em 11/05/2018].

Afilipoaie, A., Shortis, P. (2018). Crypto-Market Enforcement - New Strategy and Tactics. [Em linha]. Disponível em <http://www.swansea.ac.uk/media/GDPOSitAnalysisJune2018AfilipoaieShortis.pdf>. [Consultado em 20/05/2018].

Al-Imanm, A., Majeed, B. (2017). The NPS Phenomenon and the Deep Web: Trends Analyses and Internet Snapshots. *Global Journal of Health Science*, 9(11). [Em linha]. Disponível em <http://www.ccsenet.org/journal/index.php/gjhs/article/view/70667/38537>. [Consultado em 10/05/2018].

Aldridge, J., Décary-Hétu, D. (2014). Not an "eBay for Drugs": The Cryptomarket "Silk Road" As a Paradigm Shifting Criminal Innovation [Em linha]. Disponível em <https://poseidon01.ssrn.com/delivery.php?ID=275072007020106070124028087127125018035086055082012031067096016088068007113025001127101122106111029121027004089088031123098114109039073020059065101077106089007093068069014077008083103084021093092030068065112095014074080116106075003114110084113007086027&EXT=pdf>. [Consultado em 05/07/2018].

Barratt, M. (2012). Silk Road: eBay for drugs. *Addiction*, 107(3). [Em linha]. Disponível em <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1360-0443.2011.03709.x>. [Consultado em 12/05/2018].

Barratt, M., Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets. *International Journal of Drug Policy*, 35 [Em linha]. Disponível em <https://www.ijdp.org/article/s0955-3959(16)30227-4/abstract>. [Consultado em 12/05/2018].

BBC. (2014). Utopia drugs market forced off Tor by Dutch police. [Em linha]. Disponível em <https://www.bbc.co.uk/news/technology-26147994>. [Consultado em 16/05/2018].

Bernard, Z. (2017). Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator. [Em linha]. Disponível em <https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12>. [Consultado a 08/05/2018].

Broséus, J. et alii. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science Internationa*l, 264. [Em linha]. Disponível em <https://www.sciencedirect.com/science/article/pii/S0379073816300676>. [Consultado em 05/07/2018].

Cabral, R. (2013). Tudo sobre o Bitcoin: a história, os usos e a política por trás da moeda forte digital. [Em linha]. Disponível em <https://gizmodo.uol.com.br/tudo-sobre-o-bitcoin/>. [Consultado em 26/07/2018].

Capasso, L. (1998). 5300 years ago, the Ice Man used natural laxatives and antibiotics. *The Lancet*, 352 (9143). [Em linha]. Disponível em <https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(05)79939-6/fulltext>. [Consultado em 26/07/2018].

Chohan, U. (2017). Assessing the Differences in Bitcoin & Other Cryptocurrency Legality Across National Jurisdictions. [Em linha]. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248>. [Consultado em 26/07/2018].

Choo, K., Smith, R., McCusker, R. (2007). Future directions in technology-enabled crime: 2007–09. *Research and Public Policy Series*, 78. [Em linha]. Disponível em <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.6041&rep=rep1&type=pdf>. [Consultado em 26/07/2018].

Christin, N. (2012). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. [Em linha]. Disponível em <https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab12018.pdf>. [Consultado em 05/07/2018].

Clayton, R., Murdoch, S., Watson, R. (2006). Ignoring the Great Firewall of China. *Privacy Enhancing Technologies*, 4258. [Em linha]. Disponível em <https://link.springer.com/chapter/10.1007%2F11957454_2>. [Consultado em 07/05/2018].

Costa, A. (2017). Hélder Rosalino: A bitcoin "não é uma moeda". [Em linha]. Disponível em <https://eco.pt/2017/11/07/helder-rosalino-a-bitcoin-nao-e-uma-moeda/>. [Consultado a 10/05/2018].

Crocq, M-A. (2007). Historical and Cultural aspects of man's relationship with addictive drugs. *Dialogues Clin Neurosci*, 9(4). [Em linha]. Disponível em <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3202501/>. [Consultado em 03/05/2018].

CyberSecurity Malaysia. (2011). eSecurity Vol. 26.[Em linha]. Disponível em <http://www.cybersecurity.my/data/content_files/12/852.pdf>. [Consultado em 04/05/2018].

Daga, A. (2017). Darknet vs Dark Web vs Deep Web vs Surface Web. [Em linha]. Disponível em <https://techbuddiesbyajay.blogspot.com/2017/11/darknet-vs-dark-web-vs-deep-web-vs.html>. [Consultado em 09/05/2018].

Décary-Hétu, D., Giommoni, L. (2017). Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis Of The Effects Of Operation Onymous. *Crime, Law and Social Change*, 67(1). [Em linha]. Disponível em <http://orca.cf.ac.uk/95227/3/Hetu%20Giommoni%20-%20CLSC%20-%20Do%20Police%20Crackdowns%20Disrupt%20Drug%20Cryptomarkets.pdf>. [Consultado a 07/05/2018].

Doherty, S. (2011). Infostealer.Coinbit. [Em linha]. Disponível em <https://www.symantec.com/security-center/writeup/2011-061615-3651-99>. [Consultado em 13/05/2018].

Dolliver, D. (2015). Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal on Drug Policy*, 26(11). [Em linha]. Disponível em <https://www.ncbi.nlm.nih.gov/pubmed/25681266>. [Consultado em 15/06/2018].

El Petro. [Em linha]. Disponível em <http://www.elpetro.gob.ve/>. [Consultado em 26/07/2018].

Eleutério, F. (2006). Análise do conceito de crime. [Em linha]. Disponível em <http://www.egov.ufsc.br/portal/sites/default/files/anexos/12203-12203-1-PB.pdf>. [Consultado em 10/05/2018].

Emigh, A. (2007). The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond. *Journal of Digital Forensic Practice*, 1(3). [Em linha]. Disponível em <https://www.tandfonline.com/doi/abs/10.1080/15567280601049985>. [Consultado em 15/06/2018].

Engineering and Technology History Wiki. (2015). Milestones:Invention of the First Transistor at Bell Telephone Laboratories, Inc., 1947. [Em linha]. Disponível em <http://ethw.org/Milestones:Invention_of_the_First_Transistor_at_Bell_Telephone_Laboratories,_Inc.,_1947>. [Consultado em 15/06/2018].

Ethereum.[Em linha]. Disponível em <https://www.ethereum.org/>. [Consultado em 26/07/2018].

Europol. (2014). Operation Onymous. [Em linha]. Disponível em <https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous>. [Consultado em 19/05/2018].

Freedom House. (2017). Freedom on the Net 2017. [Em linha]. Disponível em <https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf>. [Consultado em 14/05/2018].

Fox-Brewster, T. (2016). OpenBazaar Is Not The Next Silk Road -- It's An Anarchist eBay On Acid. [Em linha]. Disponível em <https://www.forbes.com/sites/thomasbrewster/2016/03/16/openbazaar-silk-road-dark-web-drugs-ebay/#1538865a5ab4>. [Consultado em 17/05/2018].

Gillespie, T. (2018). Bitcoin price: European Union considers regulating cryptocurrency amid fears of bubble. [Em linha] Disponível em <https://www.express.co.uk/finance/city/908036/Bitcoin-price-European-Union-regulation-bubble>. [Consultado a 09/05/2018].

Godoy, G. (2015) The drug trafficking inserted in cyber space – How social networks, virtual coins, big data and software applications influence it - An analysis of the United Nations organisation [Online], Disponivel em:

<https://www.fep.up.pt/docentes/ateixeira/I2FC2015_Godoy.pdf>. [Consultado em: 17/02/2018].

Gordon, S., Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2 (1). [Em linha]. Disponível em <https://link.springer.com/article/10.1007%2Fs11416-006-0015-z>. [Consultado em 17/03/2018].

Greenberg, A. (2014). Silk Road Reduced Violence in the Drug Trade, Study Argues. [Em linha]. Disponível em <https://www.wired.com/2014/06/silk-road-study/>. [Consultado em 16/05/2018].

Hale, C. (2002). Cybercrime: Facts & Figures Concerning This Global Dilemma. *Crime & Justice International*, 18(65). [Em linha]. Disponível em <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=197384>. [Consultado em [13/04/2018]

INPUD (2014). Timeline of events in the history of drugs. [Em linha]. Disponível em <https://inpud.wordpress.com/timeline-of-events-in-the-history-of-drugs/>. [Consultado em 05/05/2018].

Jardine, E. (2015). The Dark Web Dilemma: Tor, Anonymity and Online Policing. *Global Commission on Internet Governance*, 21. [Em linha]. Disponível em <https://poseidon01.ssrn.com/delivery.php?ID=072078126116072112108017127070100086050045038009039013023072071120020102018098068104039124063013051027109080069004113005023014039057093013053122016006102080005115011041026009021107019115095076073065085090

700708500008406802907702707508202310201211912701 3&EXT=pdf>. [Consultado em 26/07/2018].

Johnson, B., et alii. (2014). Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools. *Financial Cryptography and Data Security*, 8438. [Em linha]. Disponível em <https://link.springer.com/chapter/10.1007/978-3-662-44774-1_6>. [Consultado em 13/05/2018].

Jornal de Negócios (2018). Parlamento debate proposta para transpor a directiva dos pagamentos. [Em linha]. Disponível em <https://www.jornaldenegocios.pt/economia/politica/detalhe/parlamento-debate-proposta-para-regular-pagamento-com-bitcoin>. [Consultado em 12/05/2018].

Kelso, C. (2018). Germany Treads Lightly on Bitcoin Taxation. [Em linha]. Disponível em <

https://news.bitcoin.com/germany-treads-lightly-on-bitcoin-taxation/>. [Consultado em 10/05/2018].

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy*, 9(3). [Em linha]. Disponível em <https://ieeexplore.ieee.org/abstract/document/5772960/>. [Consultado em 16/04/2018].

Lee, R., Assante, M., Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. [Em linha]. Disponível em <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>. [Consultado em 26/07/2018].

Liao, K., et alii. (2016). Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. *2016 APWG Symposium on Electronic Crime Research (eCrime)*. [Em linha]. Disponível em <https://ieeexplore.ieee.org/abstract/document/7487938/>. [Consultado em 13/05/2018].

Mancini, M. (2017). Internet das Coisas: História, Conceitos, Aplicações e Desafios. [Em linha]. Disponível em <https://pmisp.org.br/documents/acervo-arquivos/241-internet-das-coisas-historia-conceitos-aplicacoes-e-desafios/file>. [Consultado em 15/06/2018].

Martin, J. (2014) Lost on the Silk Road: online drug distribution and the 'cryptomarket'. Criminology & Criminal Justice, Vol. 14(3) 351-367.

Memoria, F. (2018). Portuguese Parliament to Discuss Cryptocurrency Payment Regulations. [Em linha]. Disponível em <https://www.ccn.com/portuguese-parliament-to-discuss-cryptocurrency-payment-regulations/>. [Consultado em 11/05/2018].

Microsoft. (2001) Virtual Private Networking: An Overview. [Em linha]. Disponível em <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10)>. [Consultado em 23/05/2018].

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Em linha]. Disponível em <https://bitcoin.org/bitcoin.pdf>. [Consultado a 08/05/2018].

Nasseri, R. (2014). An Investigation of Cryptomarkets: Assessing the Online Drugs Trade from the Perspectives of Australian Health and Law Enforcement Agencies. [Em linha]. Disponível em <https://www.researchonline.mq.edu.au/vital/access/services/Download/mq:42116/SOURCE1>. [Consultado em 16/06/2018].

National Drug & Alcohol Research Centre. (2016). Drugs and the Internet. [Em linha]. Disponível em <https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/dnetbulletin_issue7_final.pdf>. [Consultado em 16/05/2018].

Norry, A. (2018). The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin. [Em linha]. Disponível em <https://blockonomi.com/history-of-silk-road/>. [Consultado em 05/07/2018].

Nunes, L., Jólluskin, G. (2010). *Drogas e Comportamentos de Adicção: Um Manual para Estudantes e Profissionais de Saúde*. Porto, Edições Fernando Pessoa.

Nunes, L. e Sani, A. (2014). Toxicodependência e vitimação: Inquérito dirigido a indivíduos dependentes de drogas. *Análise Psicológica*, 32(1). [Em linha]. Disponível em <http://publicacoes.ispa.pt/publicacoes/index.php/ap/article/view/744/pdf>. [Consultado em 04/04/2018].

Pereira, M. (2013). Toxicodependência. [Em linha]. Disponível em <http://www.miluzinha.com/wp-content/uploads/2011/12/Toxicodepend %C3%AAncia.pdf>. [Consultado em 02/04/2018].

Pinto-Coelho, M. (1998). Toxicodependência – A liberdade começa no corpo. Fim de Século. 3ª Edição. Lisboa.

Pollock, D. (2018). Portugal Beginning Path Towards Cryptocurrency Regulation. [Em linha]. Disponível em <https://cryptocomes.com/portugal-beginning-path-towards-cryptocurrency-regulation>. [Consultado em 11/05/2018].

Potcoin. (2018). What is PotCoin? [Em linha]. Disponível em <https://www.potcoin.com/>. [Consultado em 15/05/2018].

Reed, M., Syverson, F., Goldschlag, D. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, 16(4) [Em linha]. Disponível em <https://ieeexplore.ieee.org/abstract/document/668972/>. [Consultado em 03/05/2018].

Rechtman, Y. (2017). Shifting the Risk of Cybercrime. [Em linha]. Disponível em <https://www.cpajournal.com/2017/06/19/shifting-risk-cybercrime/>. [Consultado em 20/05/2018].

Reynolds, P., Irwin, A. (2017). Tracking digital footprints: anonymity within the bitcoin system, *Journal of Money Laundering Control*, 20 (2). [Em linha]. Disponível em <https://www.emeraldinsight.com/doi/full/10.1108/JMLC-07-2016-0027>. [Consultado em 26/07/2018].

Sandre, A. (2016). Blockchain for voting and elections. [Em linha]. Disponível em <https://hackernoon.com/blockchain-for-voting-and-elections-9888f3c8bf72?gi=271d9237a274>. [Consultado em 26/07/2018].

Silva, L. (2002). Virtual Private Network - VPN. [Em linha]. Disponível em <http://www.martinsfontespaulista.com.br/anexos/produtos/capitulos/143139.pdf>. [Consultado em 22/04/2018].

Tor Project. (2018). Tor: Overview. [Em linha]. Disponível em <https://www.torproject.org/about/overview.html.en>. [Consultado em 17/04/2018].

Tor Project. (2018). Abuse FAQ. [Em linha]. Disponível em <https://www.torproject.org/docs/faq-abuse.html.en>. [Consultado em 17/04/2018].

Tor Project. (2018). Inception - Tor users. [Em linha]. Disponível em <https://www.torproject.org/about/torusers.html.en> [Consultado em 17/04/2018]

Ulrich, F. (2014). Bitcoin como investimento: uma nova classe de ativos. [Em linha]. Disponível em <https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/3466910/bitcoin-como-investimento-uma-nova-classe-ativos>. [Consultado em 07/05/2018].

Van Hout, M.C., Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, 25(2). [Em linha]. Disponível em <http://www.sciencedirect.com/science/article/pii/S0379073816300676>. [Consultado em 05/05/2018].

Wallace, B. (2011). The Rise and Fall of Bitcoin. [Em linha]. Disponível em <https://www.wired.com/2011/11/mf_bitcoin/all/>. [Consultado em 26/07/2018].

Wong, J. (2017). Bitcoin's mysterious inventor is now one of the world's 50 richest people. [Em linha]. Disponível em <https://qz.com/1159188/bitcoin-price-approaches-20000-making-satoshi-nakamoto-worth-19-4-billion/>. [Consultado a 09/05/2018].

Woody, C. (2016). What Colombian farmers can buy when they use cocaine's raw ingredient as currency. [Em linha]. Disponível em <http://www.businessinsider.com/colombia-cocaine-coca-paste-farming-trade-value-2016-6>. [Consultado em 16/05/2018].

Woody, C. (2017). Heroin is driving a sinister trend in Afghanistan. [Em linha]. Disponível em <http://www.businessinsider.com/taliban-control-of-heroin-drug-production-trafficking-in-afghanistan-2017-10>. [Consultado em 16/05/2018].

Woolf, N. (2015). Bitcoin 'exit scam': deep-web market operators disappear with $12m. [Em linha]. Disponível em <https://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars>. [Consultado em 13/05/2018].

Anexos

Primeira Parte – Questões introdutórias

1 - Idade

2 – País onde reside

Segunda Parte – Os Criptomercados

3 – Em quantos criptomercados tem uma conta de utilizador?

a) 1 b) 2 c)3 d)4 ou mais

4 – Em quantos criptomercados já realizou uma transação?

a) 1 b) 2 c)3 d)4 ou mais

5 – Quantas vezes realizou uma transação utilizando um ou mais criptomercados?

a) Menos que 3 vezes b) Entre 4 a 8 vezes c) Mais que 8 vezes

Terceira Parte – A compra

6 – Nos criptomercados, você compra ou vende drogas?

a) Compro b) Vendo c) Ambos

7 – O que adquiriu/vendeu no criptomercado? (pergunta de possibilidade de multiplas respostas)

(Dado ao largo número de drogas que podem ser vendidos, foram apenas escritos alguns como possíveis respostas e não todos, de forma a manter este exemplo simples e não condensado)

a) Marijuana b) Psicadélicos c) Cocaína e derivados d) Opióides

e) Outras drogas não descritas f) Outros produtos para além de drogas

8 – Qual é a quantidade média de droga que costuma adquirir/vender?

a) Menor que 5 doses indivíduais b)Entre 5 a 15 doses individuais

c) Mais que 15 doses individuais

9 – Qual a avaliação que faz ao produto que lhe foi vendido/aos clientes com quem lidou?

a) 1/5 b) 2/5 c) 3/5 d) 4/5 e) 5/5

10 – Considera que o produto/meio de venda é melhor do que aquele adquirido tradicionalmente nas ruas?

a) Sim b) Não c) Considero o mesmo d) Não adquiro por outros meios

11 – Quanto dinheiro já gastou/ganhou em criptomercados?

(O facto das transações serem realizadas utilizando as moedas virtuais pode alterar os valores aqui obtidos, nomeadamente pela sua volatilidade. Os valores serão colocados em Euros como exemplo apenas)

a) Menos de 100 euros b) Entre 100 a 500 euros c) Mais de 500 euros

Quarta Parte – As autoridades e outras adversidades

12 – Alguma vez teve problemas com as autoridades ou uma encomenda sua ser apreendida?

a) Sim b) Não

13 – Considera os criptomercados como uma maneira mais discreta de evitar as autoridades?

a) Sim b) Não

14 – Acha que estes serviços facilitam a vida dos consumidores e vendedores?

a) Sim b) Não

15 – Acha que estes serviços diminuem o nível de violência associado ao tráfico convencional?

a) Sim b) Não

16 – Acha que o futuro do fornecimento de drogas passa por este website?

a) Sim b) Não

17 – Na sua perspetiva, numerando de 1 a 5, 1 para não considero um factor importante e 5 para considero como um factor importantíssimo, das seguintes hipóteses, quais os que considera ser os maiores potenciais destes mercados?

a) Redução de danos

b)Comodidade

c) Menor risco em ser detetado e menor violência

d) Possibilidade de comprar diretamente aos cultivadores

e) Possibilidade de obtenção de um produto de melhor qualidade

f) Outras