Criptoanarquia

O fim do Estado como conhecemos

Rômulo I. S. Caldas

Versão gratuita distribuída pelo autor.

Compre a versão oficial se gostar do trabalho!

Versão para kindle:
https://www.amazon.com.br/dp/B01MYAYR8A/ref=pd_rhf_se_p_img_1?_encoding=UTF8&psc=1&refRID=3P2PTS9Y9AMCS4A4206V

Versão impressa: https://www.amazon.com/dp/1520435584

ISBN: 9781520435589

“A força da autoridade deriva da violência. Mas há que se admitir que, com a criptografia, nenhuma forma de violência jamais resolverá um problema matemático”

- Jacob Applebaum

ÍNDICE

1 - PRÓLOGO

A Era da Informação expande seus limites a cada segundo. Enviamos mensagens, alugamos quartos, solicitamos caronas, transferimos dinheiro, compramos produtos e contratamos uma série de serviços direto do conforto de nossas casas.

Tudo isso, é claro, depende deste complexo sistema global de comunicação que envia e traz mensagens e pacotes de informações gigantescos em poucos segundos, fazendo inveja até ao mais otimista serviço postal que um dia existiu.

Contudo, assim como na vida real, ainda estamos sujeitos à ação de pessoas má intencionadas que podem se colocar no caminho do envio ou recebimento destas mensagens e pacotes de informações para que possam usufruir ilegalmente do que quer que seja.

Assim, de forma bastante simplificada, surge a criptografia, que é um método de impor segurança a uma troca de informações ao "camuflar" as informações enviadas, dificultando ou mesmo

impossibilitando a invasão à privacidade de alguém que não esteja diretamente envolvido na troca de informações original.

Por exemplo, suponha que você envie uma carta para alguém muito especial com os dizeres "Eu te amo!", mas alguém intercepta tal carta, apaga seu conteúdo, e a reenvia com os dizeres "Eu te odeio!". Seria um absoluto desastre.

Porém, se você combinar um certo código para se comunicar com alguém e enviar uma mensagem com os dizeres "8857229Wxz!", não faria o menor sentido para um mal intencionado que interceptasse sua mensagem e isso ainda aumentaria a possibilidade de identificar que a mensagem foi violada caso a mensagem seja alterada, pois apenas remetente e destinatário saberiam desvendar o segredo.

Pense neste outro exemplo, um método de segurança popular para impedir o acesso ao seu smartphone pessoal é o estabelecimento de uma senha numérica de quatro dígitos com números que vão de zero a dez. Isso significa que o código de acesso do smartphone será um número entre dez mil possibilidades.

É um belo incentivo negativo para que alguém abandone a empreitada de tentar violar seu smartphone, porque o tempo empregado pode não valer a pena. Mas isto não seria verdadeiro para um computador moderno, que poderia desvendar essa senha sem grandes dificuldades simplesmente testando todas as possibilidades.

Isto revela uma faceta essencial dos métodos criptográficos clássicos: não são 100% seguros. Dados o devido tempo e demais recursos, é possível quebrar

uma criptografia e acessar qualquer informação.

Mas isso não é problema para o avanço tecnológico. Apesar das dificuldades em empregar este método entre grandes distâncias, já está disponível em nível comercial o uso da criptografia quântica.

Com a criptografia quântica, as informações trocadas são armazenadas e enviadas através de fótons, que são as menores partículas da luz visível. E caso um hacker tente copiar ou desvendar o conteúdo de um fóton, isso resultaria na alteração da característica física deste fóton, tornando o processo de invasão fisicamente impossível.

Assim, sendo fisicamente impossível violar uma informação em trânsito, nenhum hacker ou sujeito mal intencionado poderá causar danos durante o processo de troca de informações. Mas se é fisicamente impossível violar a informação, então o governo também não tem acesso a ela.

Desta forma, não só as grandes empresas terão acesso restrito a informações privadas, mas também os governos perderão uma enorme fatia de seu poder e soberania para lidar com questões simples, como punir caluniadores, e até mesmo questões mais complexas, como aquelas que envolvem a regulação da ordem econômica ou mesmo a cobrança de imposto de renda, conforme veremos.

2 - CRIPTOANARQUIA: MOVIMENTO POLÍTICO

"Uma maior comunicação significa que temos mais liberdade em relação às pessoas que estão tentando controlar as ideias e criar o consenso, e uma maior vigilância significa exatamente o contrário" – Julian Assange.

A popularização do acesso aos computadores e à internet no final do século XX intensificou a capacidade da humanidade para compartilhar conhecimentos e realizar empreitadas com altos níveis de eficiência.

Hoje, o poder de fazer a informação transitar o globo em questão de segundos encontra-se cada vez mais disperso nas mãos dos cidadãos comuns, e é necessário sempre ter em mente que tamanho privilégio jamais esteve ao alcance nem mesmo dos mais ricos reis absolutistas dos séculos passados.

Mensagens são trocadas, produtos e serviços são negociados, conteúdo é criado e tornado mundialmente visível em poucos instantes, empresas organizam seus processos produtivos, Estados se comunicam e criam facilidades de acessos a seus serviços. As possibilidades do uso da facilidade de troca de informações seguem crescentes.

Mas por outro lado, de forma justificada ou não, também crescem as preocupações com a questão da segurança nacional, razão pela qual Estados implementam serviços de monitoramento digital com base na argumentação da necessidade de manter em

segurança seus cidadãos.

Jacob Applebaum reconhece a possibilidade de um crescente discurso em nome da vigilância baseado no temor aos "quatro cavaleiros do Infoapocalipse": pornografia infantil, terrorismo, lavagem de dinheiro e guerra contra as drogas.

Levado ao extremo, tal tipo de argumentação pode buscar justificar mesmo a vigilância de nações aliadas, como comprovou o Wikileaks ao disponibilizar documentos que comprovam que a NSA – National Security Agency – matinha vigilância da alta cúpula da política brasileira, inclusive da própria presidência, em 2015.

O que se verifica, conforme observa Julian Assange, a mente por trás do Wikileaks, é uma constante e crescente militarização do ciberespaço, uma verdadeira ocupação militar dentro da casa do usuário enquanto ele navega tranquilamente na internet e, consequentemente, a intensificação da violação de sua privacidade.

3 – BIG DATA E VIGILÂNCIA

"Se quiser ter uma ideia do que será o futuro, imagine uma bota pisando no rosto de alguém. Eternamente" – George Orwell.

Em um dia comum, trocamos e-mails, mandamos mensagens, utilizamos mecanismos de buscas, realizamos transações financeiras, compramos e vendemos, consumimos, postamos nas redes sociais, indicamos que gostamos de algo ou que não gostamos de algo e por aí vai.

A longo prazo, nossas pegadas digitas formam uma enorme bola de neve de dados digitais contendo todas as suas ações no mundo virtual e também todas as ações das demais pessoas que utilizem quaisquer serviços online. É um verdadeiro e monstruoso montante de informações denominado *Big Data*.

De acordo com um furo jornalístico do jornal The Guardian, a NSA – National Security Agency – através de um programa de inteligência denominado Prism, tem acesso justamente aos provedores de serviços que contribuem para o acúmulo deste tipo de informações pessoais, como Google, Facebook, serviços Apple.

Tal revelação trouxe à tona o fato de outras gigantes do setor de tecnologia colaborarem com o programa *Prism*, tal como a Microsoft, desde 2007 e a Yahoo desde 2008.

Tudo isso vem a indicar total desrespeito em

relação ao vazamento indiscriminado de informações privadas para fins políticos ou comerciais quaisquer sem a autorização dos usuários e, na vasta maioria dos casos, sem nem mesmo motivo razoável para se estabelecer um sistema de vigia constante.

Por certo, a vigilância não se dá apenas por parte do Estado, pois que grandes redes sociais e sites de busca são grandes coletores de informações de uso e acesso por parte dos seus usuários com o intuito de estabelecer padrões de consumo e repassar tais informações a outros agentes econômicos de interesse.

Já no âmbito estatal, o que se passa pode ser ainda mais preocupante. O governo chinês está dando os primeiros passos para implementar um Sistema de Crédito Social que consiste em captar, por meio da tecnologia, informações de uso, acesso, consumo, etc. de seus cidadãos e implementar um ranking de comportamento, o que servirá para estabelecer o nível de acesso a crédito bancário e pontuando o cidadão de acordo com sua conduta pessoal.

Assim, os cidadãos chineses serão recompensados se agirem "bem" de acordo com a ótica ideológica definida por agentes em cargos políticos relevantes, o que contribui imensamente para estabelecer a concepção de que o indivíduo é mera engrenagem dentro da grande máquina estatal e que deve seguir os seus desígnios, comprovando que não estamos tão distantes daquilo imaginado pelas mentes por trás do seriado Black Mirror, que costuma explorar as mazelas de uma sociedade altamente tecnológica.

4 – INTERNET DAS COISAS

"Estamos presos à tecnologia quando, na verdade, tudo o que queremos são coisas que funcionem" – Douglas Adams.

A internet das coisas é a tendência tecnológica atual em conectar todas as utilidades do dia-a-dia da humanidade à internet, levando a informação a servidores que registram nossas ações, tendências, necessidades e objetivos, criando uma integração entre o mundo físico e o digital, buscando harmonizar o uso de tudo o que precisamos.

Imagine acordar e verificar em seu relógio informações como pressão cardíaca, média da temperatura corporal e dados relativos ao comportamento de hormônios no decorrer da noite, além de dados sobre sua saúde geral. Assim seu relógio pode gerar recomendações para melhora do sono, por exemplo. Imagine então que você decida sair para uma corrida, calça seus tênis, que medem seu peso e estatura, calcula quanto você correu e gera um relatório de gasto calórico e novas recomendações.

Tente imaginar que você volta para casa após a corrida e seu relógio e seus tênis cruzam informações, baseados no seu desempenho na corrida, e indicam uma refeição apropriada que você aceita, prepara e se alimenta com prazer enquanto descansa. Neste meio tempo, seus aparelhos lhe indicam uma dieta balanceada para a semana, acessam as informações da sua dispensa e notificam os

ingredientes necessários para completar a dieta ao mesmo tempo em que seu smartphone cruza informações com os supermercados nas proximidades e encontra a melhor relação de custo e benefício para as compras.

Suponha que você é então notificado e aceita ir imediatamente ao supermercado. Você então sai de sua casa e define a melhor rota a seguir no smartphone. Em seguida, encontra seu carro autônomo ligado e à sua espera. Enquanto aguarda o carro que se dirige sozinho chegar ao mercado, você paga pelas compras no caminho através do seu smartphone e um sistema de logística inteligente já lhe entrega suas compras embaladas no estacionamento do supermercado.

Incrível, não?

Agora tente imaginar que as empresas responsáveis por esta integração vendam, sem qualquer tipo de permissão, suas informações para, por exemplo, empresas de planos de saúde ou de seguro de vida que utilizarão tais informações para calcular se irão lhe oferecer um plano ou seguro com base no seu perfil ou não e, se a reposta for positiva, estipulem preços altíssimos conforme maior for o risco de vida decorrente dos seus hábitos e padrões de comportamento. Ou imagine mesmo que o governo tenha acesso a estas informações para definir se você segue um grande plano social determinado por um político qualquer ou ainda se está apto a seguir um tipo de carreira dentro do governo ou fora dele. Soa absurdo, totalitário, distópico. Uma tremenda invasão à intimidade.

Em 2016, James Clapper, então diretor da inteligência nacional, afirmou a um painel temático

perante sessão do Senado dos Estados Unidos que, no futuro, serviços de inteligência poderão usar a internet das coisas para identificar, monitorar, localizar, recrutar ou utilizar a informação de usuários para ganhar a acesso a redes.

Caso a proposta de Clapper venha a se concretizar, informações privadas estarão à mercê da vontade política de pessoas privilegiadas por estarem em altos cargos da administração política pública. Você confiaria informações tão vitais a políticos?

A menos que nossas informações digitais sejam confiadas a sistemas de proteção de dados seguros, a possibilidade de vivermos em um Big Brother na vida real é alta. A proposta chinesa relatada no capítulo anterior pode ser apenas o começo de muitas outras iniciativas de controlar as informações em níveis absolutamente invasivos e em desacordo total à vontade do usuário deste tipo de tecnologia.

5 – IDEAIS CRIPTOANARQUISTAS

"Governos do mundo industrial, seus gigantes cansados de carne e aço, eu venho do ciberespaço, a nova casa da mente. Em nome do futuro, peço a você, do passado, que nos deixe em paz. Você não é bem-vindo entre nós. Você não tem soberania onde nos encontramos" – John Parry Barlow.

Ascendendo nos anos 1990, o movimento criptoanarquista, ou cypherpunk, mostra grande preocupação exatamente quanto à questão da privacidade e vigilância tal como observamos, prezando sempre por sistemas de trocas de informação em que o anonimato seja mantido, repelindo todo e qualquer tipo de tentativa de coerção com base nos princípios matemáticos da criptografia enquanto promove a proteção de informações privadas que o usuário não deseja tornar pública. Também, para o criptoanarquista, a censura é subproduto da constante vigilância e deve ser igualmente repudiada.

A privacidade e o direito de divulgar ao restante do mundo apenas o que se desejar são tomados por absolutos e indispensáveis na construção de uma verdadeira sociedade aberta, estabelecendo um "contrato social" baseado no voluntarismo das relações civis, como ensina Eric Hughes em seu Manifesto Cypherpunk.

O criptoanarquista é aquele que acredita no

poder da criptografia para promover a mudança social e política em sua realidade. Assim, o plano de ação do movimento cypherpunk é programar. Programar e disponibilizar softwares de procedimentos criptográficos cada vez mais complexos com o intuito de proteger a transação da informação e a privacidade dos usuários, repudiando firmemente quaisquer leis que nasçam com a intenção de regular a criptografia.

Em última instância, pode se dizer que o objetivo do movimento é criar uma estrutura online inviolável, baseada no livre acordo e voluntarismo, buscando imunidade em relação às intervenções externas e desprezando a moral imposta pelo Estado, tornando suas tentativas de controle obsoletos por meio da criptografia.

Em seu Manifesto Criptoanarquista, Timothy C. May indica que, assim como a tecnologia de impressão tipográfica desbancou e reduziu o poder das guildas medievais e também a estrutura social de poder, também os métodos criptográficos irão alterar a natureza das corporações e do governo no sentido da intervenção econômica.

Em essência, conceitos legais como propriedade, expressão, identidade e movimento não se aplicam a estes pensadores. São conceitos baseados em matéria física palpável. Mas, como afirma Barlow, "não há matéria aqui".

Assim, com uma regência social deslocada do contexto impositivo estatal, esta sociedade criptoanárquica aberta, como esperam os criptoanarquistas, trabalharia para resolver problemas de interesse público de acordo com este ideário de relações espontâneas e estritamente acordadas.

Pode se dizer que o plano de ação

criptoanarquista seja uma forma de exercer aquilo que Samuel Edward Konkin III chamou de "Agorismo". O termo agorismo deriva de *ágora*, palavra grega para designar o local em que o mercado e suas atividades corriam livres.

Tal mercado não é um único lugar ou centro fixo e não só bens e serviços são vendidos, mas também informações são negociadas ou mesmo dispostas de forma livre, entendendo-se este conceito de "livre" como a total ausência de coerção.

Assim, o agorista, ou adepto do pensamento agorista, revolta-se contra toda relação social de imposição de forças e tem o dever moral de tomar as rédeas de sua vida e de suas ações, driblando leis, taxas e coerções, as mais diversas. É interessante notar que o autor considera as relações sociais como fatos regidos por princípios de mercado também, uma vez que uma pessoa escolhe como empregar seu tempo, que é um recurso econômico, em uma atividade qualquer.

Desta forma, Konkin estabelece o conceito de "Contra-Economia", que pode ser definido como toda ação humana não coercitiva cometida em desafio ao Estado, o que parece seguir a linha de pensamento moral de outros pensadores libertários, como Murray Rothbard e seu Princípio da Não Agressão, que consiste em julgar ilegítima qualquer agressão iniciada contra um sujeito pacífico que não tenha iniciado uma agressão injusta ele mesmo em primeiro lugar.

Então, estamos falando de um mundo ideal em que as implicações práticas decorrentes de desmedida liberdade parecem não ter sido devidamente consideradas, o que não significa que as aplicações que derivam desta corrente de pensamento

sejam necessariamente maléficas.

Mas, como observou Ludwig Von Mises acerca das formas de anarquia em geral, elas pressupõem um alto nível de racionalidade por parte de todos os cidadãos que devem conviver em sociedade, de forma tal que, através da razão, tal sociedade sustenta-se com base na capacidade das pessoas concluírem que a cooperação é o caminho moralmente correto e mais eficiente a ser seguido, abrindo mão da ação violenta.

Contudo, aponta Mises, "Os anarquistas deixam de perceber o fato inegável de que algumas pessoas são ou muito limitadas intelectualmente ou muito fracas para se ajustar espontaneamente às condições da vida social". Mises constata que haverá pessoas que agirão de modo antissocial e que, em decorrência disto, a sociedade anarquista seguirá à mercê destes indivíduos, exceto se a maioria das pessoas estiver "...disposta a impedir, pela ameaça ou pela ação violenta, que minorias venham a destruir a ordem social.

Entretanto, Mises parece não ter concebido a possibilidade da existência de um mundo digital em que a ameaça física não significasse absolutamente nada, pois há dificuldade, ou mesmo impossibilidade, de encontrar, no mundo físico, quem é o usuário que promove uma ação no mundo digital. A estrutura formal deste mundo digital se tornaria inviolável.

Assim, tanto a ameaça proveniente de um Estado ou de uma outra pessoa qualquer torna-se impossível. Então, pelo menos quanto à organização estrutural deste mundo digital protegido pela criptografia, a crítica de Mises quanto à possibilidade da existência pacífica deste modelo parece não se

aplicar.

6 – TECNOLOGIAS CRIPTOGRÁFICAS

"Eu não temo computadores. Temo a ausência deles" – Isaac Asimov.

Quer as pessoas se deem conta ou não, tecnologias que empreguem bases criptográficas já se fazem presentes na realidade do mundo moderno. O aplicativo de troca de mensagens instantâneas WhatsApp, por exemplo, emprega proteção criptográfica que torna as mensagens enviadas virtualmente invioláveis por quem quer que intercepte a informação.

Mas nos aprofundaremos em duas outras tecnológicas com crescente popularidade e com enorme potencial para tornar obsoleta a organização social do mundo moderno: Bitcoin e Tor.

7 – BITCOIN: A MOEDA DIGITAL

"Algo que falta, mas em breve será desenvolvido, é uma moeda virtual confiável. Um método em que, pela internet, você pode transferir fundos de A para B sem que A conheça B e vice-versa" – Milton Friedman.

Tente conceber em sua mente uma moeda que não pertença a um Estado. Ou ainda mais difícil, uma moeda unicamente virtual, sem papel impresso ou moeda cunhada. Seu valor é definido unicamente pela relação de oferta e procura daqueles que a querem adquirir, ela é irrastreável e praticamente impossível de ser ligada ao seu dono para fins jurídicos. O custo de envio desta moeda é tão irrelevante que quase não há taxas, e o alcance de dispersão é tão global e irrestrito, que não há barreira alfandegária ou fiscal que a consiga identificar e, consequentemente, regulá-la e a taxar.

Difícil imaginar? Sem dúvida. Mas já é realidade e seu nome é Bitcoin.

O Bitcoin é uma moeda virtual que veio à luz em 2008. Ele independe de uma organização estatal que a mantenha e não possui banco central ou governo responsável. O Bitcoin é sustentado por uma enorme rede de usuários dispersos por todo o mundo que emprestam o poder de processamento de seus computadores para estabelecer uma rede de segurança em torno das transações, o Bitcoin possibilita transações comerciais que flertam e caminham para a

total impossibilidade de rastreio dos envolvidos em dada transação.

Os Bitcoins, como são conhecidas as unidades desta moeda, são negociados por outras moedas tradicionais, como o dólar, real ou euro, em mercados online, como o Mercado Bitcoin ou Foxbit. As transações entre usuários são protegidas por chaves criptográficas a cada mudança de mãos das moedas, de forma que uma quantia enorme de dinheiro poderia ser transferida de uma extremidade do mundo à outra sem que se saiba quem são os envolvidos na negociação, driblando barreiras geográficas, alfandegárias, fiscais e mesmo criminais.

Estas unidades de moeda são armazenadas em "carteiras digitais", que podem ser programas de computador, apps ou mesmo uma página hospedada na internet, o que torna possível a transferência facilitada de Bitcoins de uma carteira para outra, em qualquer ponto do mundo, com poucos cliques.

Para gastar estas moedas no dia-a-dia, além da transferência direta entre carteiras digitais, o usuário pode adquirir um cartão de crédito pré-abastecido com Bitcoins, como os oferecidos pela AdvCash ou Xapo, dirigir-se a qualquer estabelecimento que aceite compras em cartão de crédito com as já conhecidas bandeiras Visa e Mastercard, conforme for o cartão escolhido, e pagar por qualquer coisa. É bastante simples.

Por meio de um sofisticado método de criptografia, supondo uma transação entre A e B, ambos os envolvidos têm chaves criptográficas distintas, que são usadas para legitimar a negociação entre eles através de chaves criptográficas públicas, registradas no Blockchain, o grande livro-razão

público do sistema Bitcoin, de forma tal que não é possível fraudar as transações ou o sistema.

Este sistema de segurança é tão seguro e prático, que bancos centrais de nações como a China e Rússia seguem estudando a possibilidade de implementarem a inovação para emitirem moedas digitais próprias.

Em decorrência da segurança e anonimato proporcionados, o Bitcoin já é referência global em práticas criminosas, como lavagem de dinheiro, compra de artefatos ilícitos e mesmo a sonegação de impostos.

Neste sentido, o Bitcoin representa uma ameaça para os já estabelecidos Estados nacionais, pois que a execução de políticas fiscais e cambiais, a criação de incentivos e estímulos econômicos, fixação de taxas de juros básico e muitas outras operações típicas de um sistema de moeda tradicional tornam-se impossíveis à medida que a população adere ao uso do Bitcoin.

No atual estado da tecnologia do Bitcoin, observa Fernando Ulrich, governos não podem inflacionar o sistema monetário emitindo mais moedas, não podem se apropriar da rede Bitcoin ou tampouco desvalorizar a moeda neste sentido.

É interessante observar que o Bitcoin não representa unicamente uma ameaça à soberania dos Estados, mas também ameaça os enormes monopólios e conglomerados bancários, uma vez que a necessidade de ter uma conta em um banco tende a ser extinta à medida que as pessoas resolvam a aderir à economia centrada no Bitcoin.

Mas não só por isso. Soluções de empréstimos de dinheiro direto entre usuários e com o uso de

Bitcoin, tais como o BTCJam ou Bit Lending Club, já são uma realidade e operam a intermediação destes empréstimos longe das mãos dos sistemas bancários, que também parecem caminhar em direção à obsolescência.

8 – TOR: NAVEGAÇÃO ANÔNIMA

"Nunca seremos capazes de acabar com o anonimato de todos os usuários do TOR o tempo inteiro" – National Security Agency.

Suponha, por um instante, que você adquira a habilidade mágica de sair pelas ruas de qualquer cidade do mundo protegido por uma capa de invisibilidade, podendo ver o que quisesse e se comunicar com quem quisesse sem poder ser identificado. Perigoso? Instigador? Curioso? Provavelmente todas as alternativas. E adivinhe, você já pode fazer isso na WEB.

TOR - The Onion Router – é um navegador baseado em uma rede de servidores de internet voluntários, que são os outros usuários, mais conhecida por ser uma porta de acesso à Deep Web, parte "escondida" e obscura da internet convencional em que é possível, por exemplo, contratar assassinos de aluguel.

Há também usos legítimos para o TOR: o navegador é empregado por jornalistas, dissidentes políticos, whistleblowers – como Julian Assange, conhecido por seus vazamentos através do Wikileaks - e pela Marinha dos Estados Unidos para operações de segurança. A Deep Web também é conhecida por seus intermináveis acervos de livros raros, manuais técnicos, materiais didáticos, manuscritos, artigos e trabalhos acadêmicos, todos disponíveis gratuitamente para download para quem souber

procurar.

O TOR está, semelhante ao Bitcoin, a poucos cliques de distância de qualquer pessoa com acesso à internet. Ao baixar, instalar e abrir a rede TOR, diretamente, gratuitamente e sem restrições, a partir do site que o desenvolve, o usuário conecta-se a uma extensa rede de "nós" digitais. Ao se conectar a um nó, seu IP, espécie de endereço digital do computador, passa a ser protegido por criptografia enquanto um IP diferente do inicial é "emprestado", e este último conecta-se a um novo nó, em um longo caminho de mais nós, mais criptografia e novos IPs, até alcançar a informação inicialmente solicitada pelo usuário.

Este sistema de anonimato é um grande empecilho para o controle do tráfego de dados e identificação de usuários. No documento intitulado *Tor Stinks*, fruto dos vazamentos de Edward Snowden – ex analista da NSA – a Agência de Segurança Nacional deixa claro que: "Nunca seremos capazes de acabar com o anonimato de todos os usuários do TOR o tempo inteiro".

A resposta ao vazamento deste documento não tardou, pois logo seguiu o anúncio dos desenvolvedores do TOR de que é necessário que a comunidade da internet continue trabalhando para melhorar a segurança dos navegadores para que eventuais brechas de segurança sejam corrigidas.

À medida que tais tecnologia venham a possibilitar formas mais seguras de anonimato, será crescente a preocupação com a segurança nacional em relação a diversas práticas criminais, mas também será nulo o poder de quem quer que seja de, por exemplo, controlar e moldar conteúdo midiático ou conter a

liberdade de expressão.

Estamos falando, sem dúvida, de uma faca de dois gumes: a proteção criptográfica permite amplo acesso e liberdade, mas sob o constante risco de abusos e libertinagem. Mas tais tecnologias não deixam de ser artefatos menos revolucionário em decorrência disto.

9 - SILKROAD: ESTUDO DE CASO

"Eu sei que este mercado é baseado unicamente na confiança em que vocês depositam em mim e eu não tomo isso por garantido. É uma honra servi-los e mesmo que vocês não saibam quem sou e não tenham recursos para contestar caso eu traia vocês, espero que, com o tempo, eu tenha mais oportunidades para demonstrar que minhas intenções são genuínas e que nenhuma quantidade de dinheiro pode comprar minha integridade" – Ross Ulbricht.

Imagine que um dia você saia de casa protegido pela capa de invisibilidade do capítulo passado, vá até um mercado secreto onde só entra quem estiver protegido por outras capas de invisibilidade e se depare com uma série de prateleiras vendendo alucinógenos, vários tipos diferentes de maconha, estimulantes neurais, e uma infinidade de produtos nesse sentido. Nesse mercado secreto, você escolhe algo e paga em dinheiro impossível de rastrear.

Insano? Talvez sim. Impossível? Certamente não. Mas você não precisa sair de casa para fazer isto.

Atuando como centro de comércio ilegal na Deep Web – acessível via TOR – entre os anos de 2011 e 2013 e intermediando o comércio de artefatos ilegais de drogas como maconha, ecstasy, derivados do ópio, drogas psicodélicas e afins, o site Silk Road movimentou precisas 9.519.664 moedas de Bitcoins,

algo em torno de U$D1,3 bilhões, valor estimado em 18 de outubro de 2013 de acordo com a cotação da moeda.

Eventualmente, os responsáveis pelo site foram pegos, e segundo a juíza encarregada, Katherine Foster, este foi um caso sem precedentes na história, pois foi a primeira vez que o crime "lavagem de dinheiro" foi relacionado a uma moeda digital, o Bitcoin.

Durante o processo, a questão do quão longe o governo pode ir para descobrir identidades online impulsionou a defesa a questionar se o processo baseou-se em uma invasão de computadores, por parte da polícia, sem mandato algum. A promotoria alegou, contudo, que teve sorte ao encontrar um erro na página do Silk Road, que vazou o IP do responsável pelo site, ligando Silk Road a Ross Ulbricht, identificado como autor da página.

E mesmo com todo este trabalho para impedir a operação do Silk Road, em 15/01/2017 – data da escrita deste trecho – encontravam-se em perfeito funcionamento dois substitutos do Silk Road na Deep Web, podendo ser acessados, por meio do navegador TOR, pelos links "reloadedudjtjvxr.onion" e "http://cryptomktgxdn2zd.onion/signin.php".

Também o próprio sistema de trocas do Bitcoin segue suas operações em âmbito global, possibilitando a realização de transferências de valores, legais ou não, de forma que apenas os envolvidos na transação tenham ciência do que acontece de fato.

Veremos então, de forma breve, o que é e como se comporta a criptografia.

10 - CRIPTOGRAFIA

"Operações secretas são essenciais na guerra; os exércitos se baseiam nelas para dar cada passo" – Sun Tzu.

A criptografia acompanha a história da humanidade já há bastante tempo. Na Antiguidade romana, Júlio César empregava um método de segurança em sua troca de mensagens que passou a ser conhecido como a "Cifra de César". Através deste método, destinatário e remetente combinariam previamente o código para decifrar uma mensagem, que consistia em saber quantas vezes uma letra seria deslocada e substituída por outra no alfabeto para mascarar a real mensagem.

Desta forma, se o número escolhido fosse três à frente, então todo "A" na mensagem original deveria ser substituído por uma letra três vezes à frente de "A" no alfabeto. Seria um "D". Preservando o fator três para a troca de letras, se você quisesse enviar a mensagem "Mande uma legião ao Rubicão imediatamente", a mensagem criptografada seria "Pdqgh xpd ohjlãr dr Uxelfãr lphgldwdphqwh".

Avançando bastante no tempo, especificamente na década de 1920, Arthur Scherbius, um engenheiro alemão, desenvolveu "Enigma", máquina de troca de mensagens protegidas por criptografia e que passou a ser usada pelas forças militares alemãs na Segunda Guerra para definir e compartilhar estratégias.

Então, um tremendo esforço de guerra foi feito pelos britânicos em uma tentativa de desvendar os segredos do Enigma e virar a mesa durante a guerra, resultando no desenho da Bomba Eletrônica, ou simplesmente Bombe, por Alan Turing. Mais tarde, a máquina foi aperfeiçoada por um time de criptoanalistas e engenheiros.

Alan Turing, reconhecido como pai da computação, concebeu o primeiro modelo abstrato de um computador aos 24 anos de idade e liderou a primeira equipe a produzir o primeiro computador digital a existir em 1943, o Colossus.

Turing não só decifrou os segredos da máquina que mudou o curso da Segunda Guerra, mas também instalou as bases para a chegada de um novo tipo de tecnologia que viria a elevar a complexidade dos processos criptográficos a níveis nunca antes imaginados.

11 – CRIPTOGRAFIA CLÁSSICA: SIMÉTRICA E ASSIMÉTRICA

"Vivemos em uma sociedade primorosamente dependente de ciência e tecnologia, mas em que poucas pessoas sabem alguma coisa sobre ciência e tecnologia" – Carl Sagan.

As técnicas modernas de criptografia se dividem em simétrica e assimétrica. Na criptografia simétrica, similar à Cifra de César, quem envia a mensagem e quem a recebe combinam previamente qual será o código, ou a chave, responsável por alterar a mensagem original, bastante aplicar o código de forma reversa na mensagem alterada para se chegar à mensagem original.

No âmbito da criptografia simétrica, temos algoritmos, que são basicamente uma receita de como fazer algo, tais como o DES – Data Encryption Standard – que utiliza chaves criptográficas de 56 bits, o que significa que a chave é uma única possibilidade entre 2 elevado a 56, exatas 72,057,594,037,927,936 possibilidades. São 72 quadrilhões de possibilidades.

Contudo, esse nível de proteção certamente não é garantia de inviolabilidade. Caso surja alguém com recursos o suficiente, poderá tentar quebrar esta proteção criptográfica simplesmente tentando todas as possibilidades possíveis, o que foi feito em uma competição em 1988, provando a relativa falta de segurança em sistemas que contavam com este tipo de proteção.

Desde então, novos algoritmos criptográficos vieram à luz, tal como o AES – Advanced Encryption Standard – que conta com a possibilidade de criptografia de até 256 bits, o que equivale a dizer que a solução para revelar uma mensagem criptográfica é uma em 2 elevado a 256 possibilidades, um número absurdamente grande demais. Tente fazer na calculadora e se assuste!

Porém, a chave simétrica requer que as pessoas envolvidas no processo de comunicação repassem o segredo da criptografia antes do envio da própria mensagem, o que representa um grande risco de segurança durante este processo de comunicação. Seria como enviar um cofre para alguém contendo uma mensagem secreta dentro. Contudo, antes do envio do cofre, é necessário enviar uma carta comum a esta pessoa com o segredo do cofre escrito para que ela possa desvendá-lo.

Por outro lado, tem-se um diferente tipo de sistema de proteção criptográfico, conhecido como criptografia assimétrica. Através deste método, a pessoa "A" cria duas chaves: uma pública e uma privada. A chave pública é enviada para qualquer um que queria enviar mensagens para a pessoa "A", que só consegue decifrar a mensagem enviada utilizando sua chave privada, que não foi comunicada a ninguém. Neste sistema, nem mesmo a pessoa que envia a mensagem terá acesso a ela posteriormente, somente o receptor que possui a chave privada.

Um dos métodos de criptografia assimétrica mais conhecidos é o RSA, que consiste em estabelecer chaves privadas e públicas a partir da multiplicação de dois números primos enormes, lembrando que primo é o número divisível apenas por um e por ele mesmo.

A partir do resultado dessa multiplicação, a quebra da criptografia dar-se-á com a tentativa de fatorar este número multiplicado, lembrando que fatorar é encontrar os números primos que resultaram na multiplicação em questão.

A dificuldade em quebrar este tipo de criptografia encontra-se justamente no uso de números primos muito extensos. Experimente, por exemplo, fatorar o número 944.871.823.102.126.331 até encontrar os números primos que lhe deram origem em uma multiplicação (982.451.653 x 961.748.927).

E este não é um número grande para este tipo de método de criptografia. A RSA Data Security, que é responsável pela padronização do RSA recomenda que chaves de 2048 bits sejam usadas. Isso significa usar números primos de ao menos 617 dígitos como forma de garantir que as chaves não sejam quebradas pelo menos até o ano de 2030.

Então, em tese, alguém teria de deixar um computador calculando as possibilidades de quebra de uma chave de criptografia durante anos para que isso venha a acontecer. Dentro da realidade de recursos limitados que a maioria das pessoas e todos os governos enfrentam, certamente não há como se empenhar para promover uma quebra para cada indivíduo que fizer uso deste tipo de criptografia, e já é bastante inviável buscar quebrar a proteção de um indivíduo sequer.

Em todo caso, é certo que a criptografia clássica pode ser quebrada e tem de ser aperfeiçoada à medida que a capacidade de processamento dos computadores aumenta ao longo dos anos, pois isso também faz aumentar a capacidade destes mesmos

computadores de quebrar proteções criptográficas com maior facilidade, isso para não dizer que, quando os computadores quânticos viáveis povoarem a terra, desvendar esse tipo de criptografia clássica será brincadeira de criança.

Mas será possível uma criptografia impossível de ser violada?

12 – CRIPTOGRAFIA QUÂNTICA

"As máquinas me surpreendem com muita frequência" – Alan Turing.

Gravando informações em fótons, as menores partículas da luz visível, a informação protegida por criptografia quântica pode fazer o uso da geração aleatória de chave criptográfica para cada mensagem enviada – *One Time Pad* - tornando inviável a identificação de um padrão no envio de mensagens e, consequentemente impedindo a quebra da criptografia.

Funciona assim: seu computador grava a informação no fóton e o polariza de forma aleatória. O receptor da mensagem possui diferentes detectores polarizados capazes de identificar o fóton e reconhece-lo enquanto informação digital, transformando os fótons em bits.

Acontece que os detectores polarizados agirão de forma aleatória no reconhecimento dos fótons, razão pela qual, após o receptor ter transformado as informações em bits, ele se comunica com quem enviou a mensagem e diz qual detector usou para perceber o fóton, eliminando aquilo que estiver errado baseando no envio original dos fótons, o que termina com o destinatário da mensagem tendo em mãos a chave criptográfica para decifrar uma única mensagem a ser enviada.

Assim, a ordem correta dos detectores polarizados mantém-se pública, mas nada pode ser feito sem os fótons polarizados enviados diretamente

ao destinatário da mensagem, mas acontece que não só os fótons não seguem qualquer padrão de polarização, como a tentativa de interceptar um fóton em seu caminho para o destinatário original usando o detector errado altera as características físicas deste fóton e possibilita a identificação de uma tentativa de interceptação da mensagem.

E este é justamente um dos problemas em se implementar o uso da criptografia quântica: pequenos distúrbios podem alterar completamente a característica dos fótons, o que dificulta o uso desta tecnologia entre grandes distâncias.

Entretanto, trata-se de um sistema de proteção criptográfica fisicamente impossível de ser violado, o que poderia potencializar o uso de tecnologias como o TOR e Bitcoin a um patamar de total e inviolável segurança e anonimato, gerando implicações com potencial para causar uma enorme ruptura na organização social deste início do século XXI.

13 – LIBERDADE, IGUALDADE E FRATERNIDADE

"Segundo a visão libertária, o único papel da violência é a defesa da pessoa e de sua propriedade contra outra violência. Qualquer uso da violência que vá além da defesa é, em si mesmo, agressivo, injusto e criminoso" – Murray N. Rothbard.

Além de servir como instrumento que visa a impedir o avanço da vigilância e militarização do ciberespaço, impedindo a apropriação de dados pessoais privados, a possibilidade da inviolabilidade de estruturas econômicas de mercado e livre comércio e mesmo acesso a informações privadas por parte de um órgão centralizador ou de terceiros com vantagens e privilégios sobre os demais certamente é solo fértil para a associação e proliferação de ideologias libertárias que primam, em várias medidas, pela liberdade individual em um crescente cinismo e desconfiança em relação à atuação estatal.

Tecnologias como o Bitcoin tornam a fiscalização da renda e a consequente cobrança de impostos um enorme empecilho para o Estado, que tem limitados recursos para estabelecer o vínculo jurídico necessário para impor a obrigação da cobrança do imposto de renda sobre um cidadão qualquer. Isso, por si só, já mina a atuação estatal, necessariamente dependente das contribuições tributárias para manter funcional sua administração. Assim, o Estado tem seu poder fragmentado e torna-

se refém, cada vez mais, de contribuições voluntárias.

Para citar um outro exemplo de como o Estado tende a perder sua relevância com o avanço tecnológico da criptografia, sistemas descentralizados de distribuição e compartilhamento de informação já são um grande empecilho para que o Estado consiga garantir e preservar direitos autorais. Adicionando proteção criptográfica de anonimato a esse tipo de rede, haveria impossibilidade mesmo em reconhecer o que está sendo pirateado ou mesmo se algo está.

Em um ciberespaço com estrutura de proteção à identidade e ações econômicas anônimas protegidas e invioláveis, todos os que adentrarem a este recinto só poderão fazê-lo em condições de paridade em relação aos demais, com o mesmo grau de liberdade dos demais, partilhando, enfim, do mesmo grau de igualdade dentro deste sistema formalmente estruturado.

Frédéric Bastiat observa que não é possível compreender a fraternidade legalmente forçada sem que a liberdade seja legalmente destruída e a justiça seja legalmente pisada. Neste âmbito tecnológico em que as propriedades físicas da matéria – como os fótons – tornam a violabilidade individual fisicamente impossível, surgirá espaço para que a fraternidade, em sua forma mais pura por não ser compulsória, se manifeste.

Neste sentido, em 13 de abril de 2015, em um pedaço de terra de 7 quilômetros quadrados fora proclamado o terceiro menor Estado soberano do planeta, maior apenas do que o Vaticano ou Mônaco. Não foi uma revolução, não houve conflito. O pequeno território, localizado entre a Sérvia e a Croácia, não fora proclamado por nenhuma destas ou

outras nações e deixou de ser *terra nullius*, ou terra de ninguém, quando três amigos libertários se reuniram e declararam a soberania da República Livre de Liberland.

Tendo ideais libertários em sua fundação, Liberland tem o Bitcoin como sua moeda oficial, e sua constituição prevê a impossibilidade do planejamento econômico centralizado em decorrência da falta de cobrança compulsória de impostos aos cidadãos.

O Estado de Liberland tem a pretensão de se sustentar apenas com base em contribuições voluntários de seus habitantes e, segundo as palavras do presidente da nação, Vit Jedlicka, "Bom, se ninguém pagar, não haverá país".

Com o emprego de proteção criptográfica e anonimato esse tipo de realidade tem o potencial para se revelar uma tendência nos anos que estão por vir. Uma outra tendência fundada nestas mesmas possibilidades e que já é uma realidade para os cidadãos de Liberland é a existência do conceito de E-residência ou residência virtual. Por meio de um aplicativo para Android e iOS publicado pela República Livre de Liberland, os e-cidadãos registrados fazem parte de um integrado sistema entre Uber, Fiver, Aibnb e Ebay, Facebook e LinkedIn onde todos podem oferecer serviços baseados em sua localização de GPS.

Contudo, as normas a reger as interações entre clientes, produtores e prestadores de serviços do aplicativo possuem o lastro legal do sistema jurídico de Liberland, de forma que, com alcance global e de forma voluntária, qualquer um pode optar por um sistema legal diferente para protegê-lo em dada

situação, não importando em que país esteja.

Estas múltiplas facetas das possibilidades trazidas pelo avanço tecnológico nos servem como prenúncio para indicar que as relações sociais estão em um período de transição que pode alterar toda a organização estatal conforme conhecemos.

14 – EPÍLOGO: O FIM DO ESTADO COMO CONHECEMOS

"Nós estamos criando um mundo em que todos podem entrar, sem privilégios e sem preconceitos raciais, econômicos ou preconceito de nascimento e sem força militar" – John Parry Barlow.

A criptografia representa uma enorme ruptura para toda e qualquer atuação do Estado. Tomando apenas tecnologias como o navegador TOR e aliando-o à transação de Bitcoins, um cidadão comum pode, a partir de alguns poucos comandos, fazer valores exorbitantes transitarem globalmente, de forma anônima e segura. Os custos e o tempo necessário para que um Estado venha a, através de sua polícia, violar as proteções criptográficas simplesmente não se justificam. O Estado tem recursos limitados, e dedicar uma série de computadores por tempos tão longos que podem chegar a anos para lidar com um indivíduo que seja não é razoável.

Isso traz à tona a consequências contundentes do emprego deste tipo de tecnologia: impossibilidade de estabelecer vínculos, para fins jurídicos, entre quem comete o crime, o crime cometido, os resultados deste crime e o local físico onde o crime foi realizado e surtiu efeitos.

Isto resulta na flexibilização do poder coercitivo do Estado que segue intimamente dependente e condicionado a um conceito de territorialidade e jurisdições que vem se provando

impróprio, senão completamente incapaz, para lidar com novas tecnologias. O Estado caminha para a obsolescência quanto à aplicação de suas leis à medida que inovações baseadas em criptografia são incorporadas ao cotidiano.

Hoje, através do sistema monetário convencional, o Estado pode intervir na ordem econômica de três maneiras: criando leis e as impondo com seu poder de polícia; criando incentivos e estímulos fiscais e demais regulamentações; e atuando empresarialmente, como se fosse apenas mais uma pessoa agindo no mercado. Mas com a crescente busca pelo Bitcoin e alternativas digitais não vinculadas a uma nação, o Estado não tem opção, senão aceitar participar do sistema econômico como um mero indivíduo no meio dos demais.

De forma similar, a criação de incentivos e estímulos, execução de políticas fiscais e cambiais, emissão de moeda, fixação de taxas de juros básico e muitas outras operações típicas de um sistema financeiro moderno tradicional também tendem à impossibilidade, estabelecendo uma estrutura de organização econômica em que todos os participantes do mercado não tenham privilégios ou regalias para influenciar no andamento destes mercados.

Assim, o Estado tenderá a exercer cada vez menos controle em sistemas protegidos por criptografias avançadas, ou outras tecnologias que o valham, resultando na constante fragmentação do poder soberano dos Estados.

Isso tudo se concluiu tomando por base apenas duas tecnologias atreladas à criptografia e ao anonimato: TOR e Bitcoin. É necessário ainda levar

em consideração que estas tecnologias são relativamente novas e outras tantas ainda estão em desenvolvimento.

Vivemos em uma era de transição conhecida como a "Internet das coisas". Especula-se que, em breve, até o mais banal dos eletrodomésticos esteja conectado à internet, gravando dados e buscando estabelecer um padrão de comportamento para melhor servir e atender aos consumidores.

Com isso, é bem provável que toda nossa rotina, nossos gostos, o que pesquisamos nos sites de busca, o que compramos, quando compramos, para quem compramos, o que lemos, o que nos interessa, o que acreditamos, nossas ideologias, como nos relacionamos e muitas outras informações extremamente pessoais estejam disponíveis em um servidor obscuro, à venda sem restrições para o maior pagador ou disponível para os governos fazerem o que bem entenderem.

Até lá, temos a oportunidade de evitar que isso de fato venha a acontecer. Podemos contribuir de inúmeras formas para o desenvolvimento de tecnologias de proteção ao anonimato e segurança on-line. Você pode desenvolver, testar, financiar, informar-se e informar aos demais, pois a guerra pela privacidade já está sendo travada na rede há muitos anos.

Ao mesmo tempo, não podemos fechar os olhos às possibilidades imorais que acompanham o avanço criptográfico, como a proliferação da pornografia infantil e o terrorismo. É igualmente necessário procurar soluções para estes enormes problemas.

Em suma, para o movimento criptoanarquista,

as enormes instituições jamais devem ter poder irrestrito e imparável sob o cidadão, que é pequeno em comparação. Entretanto, não é uma questão de viver em segredo, é uma questão de ter o poder de decidir o que e quando revelar alguma informação sem permanecer refém das intenções de megacorporações ou de Estados gigantes, constantemente lhe dizendo como agir em cada âmbito da vida privada, ou utilizando dados privados em má fé para alcançar algum objetivo qualquer. Se você acredita nisso, você é um criptoanarquista.

SOBRE O AUTOR

Rômulo I. S. Caldas é um entusiasta da tecnologia e estudante de Direito que, na data da confecção deste livro, encontra-se no quarto período do curso.

E-mail para contato: romuloiscaldas@gmail.com