Cypherpunks: Caminhando por uma Estrada Orwelliana[1]

Felipe da Silva BERNARDO[2]
Bruno Ribeiro NASCIMENTO[3]
Universidade Federal da Paraíba, João Pessoa, PB.

RESUMO
O objetivo desse trabalho é analisar o movimento *cypherpunks*: ativistas digitais que acreditam na utilização da criptografia e de métodos similares a fim de provocar mudanças sociais, políticas e econômicas. Nesse sentido, debateremos sobre a questão da vigilância da vida civil feita por governos e empresas por meio das tecnologias de informação e comunicação e toda rede telemática. Veremos como a rede mundial de computadores tem uma vertente dupla, ou seja, o mundo do ciberespaço pode ser utilizado tanto para limitar nossa privacidade quanto para burlar a imposição dos meios de comunicação de massa que verticalizam a informação.

PALAVRAS-CHAVE: *cypherpunks*; criptografia, ciberespaço; vigilância.

DEFINIÇÕES E BREVE HISTÓRICO DO TERMO *CYPHERPUNKS*

No dicionário Oxford, o termo *Cypherpunks* define o movimento que lança mão da criptografia quando acessa uma rede de computadores a fim de terem a privacidade protegida. Em outras palavras, o objetivo do movimento é garantir à privacidade, especialmente contra autoridades governamentais e empresas privadas no ciberespaço (OXFORD, 2014). Os *Cypherpunks* acreditam que criptografia de forte algoritmo irá capacitar os indivíduos a se comunicarem com segurança e liberdade. Por isso, eles se opõem a qualquer tipo de regulamentação governamental da criptografia (WHATIS.COM, 2014).

O termo foi criado no final de 1992 pela *hacker* Jude Milhon, conhecida no mundo virtual como Stª Jude. Escritora, programadora e uma das fundadoras do movimento *Cypherpunks*, Stª Jude fez um trocadilho entre as palavras *cypher*, referente à criptografia e *ciberpunk*, um dos subgêneros da ficção cientifica que trata de histórias que envolvem um futuro problemático e sombrio onde as tecnologias de informação e da cibernética são empregadas por governos e organizações totalitárias, tendo a rede mundial de computadores como uma das dominadoras de todos os aspectos da vida dos cidadãos (WIKIPÉDIA, 2014a).

A criptografia nasceu aproximadamente na década de 1970 com o objetivo de manter em segredo informações de extrema relevância. Era empregada por agências militares, do governo e de espionagem. De acordo com Dertouzos (1997, p. 138), a criptografia é

[1] Trabalho apresentado no DT 6 – Rádio, TV e Internet do XVI Congresso de Ciências da Comunicação na Região Nordeste realizado de 15 a 17 de maio de 2014.

[2] Graduando do curso de Comunicação em Mídias Digitais pela UFPB. E-mail: bernardofeli@gmail.com

[3] Mestrando em Comunicação e Culturas Midiáticas pela UFPB. E-mail: RN.brunno@gmail.com

responsável por "misturar ou codificar a informação, de modo que usuários não autorizados dificilmente consigam entender o significado, e que os destinatários possam reorganizar ou decodificar o material de modo simples". Inicialmente o uso de criptografia avançada em computadores foi dominado pelo Estado até meados dos anos 80. O cenário começa a mudar quando desenvolvedores independentes passam a criar seus códigos a fim de privarem suas informações de possíveis interceptações ou de alguns "prováveis" curiosos.

Dessa forma, surgem os primeiros ativistas que, contrários a vigilância, passaram a desenvolver e distribuir seus sistemas de criptografia. Assim, as pessoas que quisessem manter seus dados, e-mails e arquivos no computador e ao mesmo tempo protegidos de olhares externos, poderiam fazê-lo utilizando programas como *PGP* de criptografia assimétrica. O PGP, por exemplo, teve rapidamente seu código e programa disponibilizado na internet para *download*. O programador do código era um americano: Philip Zimmermann. Ele foi acusado pelo governo dos Estados Unidos por violação do direito de exportação de software de criptografia nacional. Zimmermann se defendeu afirmando não ter publicado o código-fonte do programa fora do território americano, mas o fez em livros, consciente de que a Legislação Americana garantia liberdade de expressão para as publicações impressas.

Para nossos objetivos, o importante é saber que as ações contra Zimmermann motivaram investidas dos governos americanos e de países europeus em controlar o uso e domínio sobre a criptografia. Essas tentativas de controle governamental acabaram unindo várias pessoas em busca do uso da escrita cifrada, tendo como uma de suas principais conseqüência a criação do movimento *Cypherpunk*. Foi criada assim um *mailing list* a fim de debater questões como privacidade, monitoramento do governo e controle corporativo de informações. Esse *mailing* iniciou em 1992, e tinha várias discussões técnicas que envolviam criptografia, matemática, ciências da computação, política, comunicação e filosofia (WIKIPÉDIA, 2014a). Em 1994, o *mailing* chegou a conter 700 pessoas.

Dessas discussões, o matemático Eric Hughes criou em 1993 o "Manifesto de um Cypherpunk". Nele, são combinadas várias idéias e discussões envolvendo o espírito de individualismo no ciberespaço, o uso de criptografias para preservar a privacidade das pessoas, a necessidade de manter privacidade em uma sociedade aberta, entre outros conceitos. As idéias básicas do manifesto de Hughes (1993) são as seguintes[4]:

[4] Traduçãolivre. Original: "Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. […].We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy […].We must defend our own privacy if we expect to have any […].We know that someone has to write software to defend privacy, and we're going to write it.

> A privacidade é necessária para uma sociedade aberta, na era eletrônica. Privacidade não é segredo. Um assunto privado é uma coisa que alguém não quer que o mundo inteiro saiba. Um segredo é uma coisa que alguém não quer que ninguém saiba. A privacidade é o poder de revelar-se seletivamente para o mundo [...]. Não podemos esperar que os governos, corporações e outras grandes organizações nos garantam privacidade como uma espécie de caridade [...]. Devemos defender nossa própria privacidade, se planejamos ter alguma [...]. Cypherpunks escrevem códigos. Nós sabemos que alguém tem que fazer software a fim de defender a privacidade, e como não se pode realmente ter privacidade a não ser que todos a tenham, nós mesmos vamos fazer o software (HUGHES, 1993).

O movimento atingiu seu auge durante esse período dos anos 90 com as "criptoguerras" e as várias tentativas de restringir o uso da criptografia feitas pelo governo. Além disso, o movimento ganha mais força em 2011, na Primavera Árabe, após a censura da internet nos países envolvidos. Em 2013, Jullian Assange, escritor do livro "Cypherpunks: liberdade é o futuro da internet", discutiu com outros três ativistas do mundo digital – Jacob Appelbaum, desenvolvedor do software de criptografia TOR; Andy Muller-Maguhn, porta voz do grupo *haccker Chaos Computer Club*; e Jéremie Zimmermann, ativista da ONG *La Quadrante du Net* – o futuro do movimento. O livro de Assange apresentava como idéia principal a defesa da utilização da criptografia pela sociedade civil a fim de manter em sigilo informações que fossem consideradas importantes pelas pessoas. Apresentando os riscos de um mundo onde os metadados privados são sistematicamente coletados e acessados pelas vigilâncias governamentais e empresariais do ramo tecnológico.

Mesmo reconhecendo a existência da pornografia infantil, lavagem de dinheiro, tráfico de drogas e terrorismo – os chamados "Quatro Cavaleiros do Infoapocalipse" – os *Cypherpunk* admitem que exista a real possibilidade de criminosos virtuais e terroristas explorarem o uso de sistemas de criptografia forte no ciberespaço para fins não éticos. No entanto, eles aceitam esse tipo de risco como preço a ser pago pelo direito do indivíduo e da sociedade civil à privacidade (WHATIS.COM, 2014).

CULTURA DAS MÍDIAS E A QUESTÃO DA VIGILÂNCIA

Se as novas mídias possibilitaram inicialmente aos cidadãos comuns o poder de produzir, expressar e divulgar conteúdo a fim de reivindicar seus direitos, ela também permite a destruição, o vandalismo e o roubo. Como diz Santaella "na web vivemos entre os anjos e as bestas"[5]. O século XX passou por uma revolução informacional com o aparecimento de novos meios de comunicação. Desde a metade da década de 70, e principalmente nos anos 90, quando os meios de comunicação eram caracterizados principalmente por sua horizontalidade,

[5] https://www.youtube.com/watch?v=vzlhvVHLE1s

até o advento do ciberespaço, que proporcionou uma re-significação e uma re-definição dos pólos de recepção e de produção, é possível perceber como o mundo digital revolucionou nossa sociedade. Computador, E-mail, celular, sites, internet, TV a cabo e webcams possibilitaram uma vasta diversidade de novos caminhos comunicacionais.

Para Thompson (2009), o uso midiático na sociedade "implica a criação de novas formas de ação e de interação no mundo social, novos tipos de relações sociais, novas maneiras do individuo com os outros e consigo mesmo" (THOMPSON, 2009, p. 13). Isso porque a mídia altera de maneira fundamental a organização social e temporal de uma sociedade que não estão mais ligadas ao compartilhamento de um local comum.

Esse processo se dá porque os meios de comunicação são meios de produção e difusão de formas simbólicas no espaço e no tempo. Essa transmissão acontece através de algum meio técnico ou substrato material com a capacidade de fixar ou preservar uma determinada informação, reproduzi-la em larga escala, permitindo assim o distanciamento de um dado conteúdo simbólico do seu contexto de produção (THOMPSON, 2009). Aliás, pode-se dizer que essa é uma das principais características dos meios de comunicação social: eles têm a capacidade de dissociar os produtos simbólicos de seu ambiente físico-temporal, bem como fazer com que as pessoas possam ter contato com determinado tipo de conteúdo ainda que não partilhe do mesmo contexto espaço-temporal em que esse último foi produzido.

No entanto, apesar de toda essa ambiência diferente criado pelos meios de comunicação, a centralização e o controle desses meios, principalmente dos que dependem da internet, criaram um ambiente propicio à vigilância. Ou seja, ganhamos um maior poder de comunicação, ao mesmo tempo em que estamos mais vigiados – preço que aprendemos rapidamente a pagar. Passamos a viver sob um constante "estado de vigilância" sobre nossos atos, ou seja, o ciberespaço potencializa uma privacidade cada vez mais frágil. "É possível usar a tecnologia da informação para atacar nossa privacidade, mas também para protegê-la" (DERTOUZOS, 2002, p. 135).

Ao ir às compras, viajar, buscar no Google, comprar no Mercado Livre, baixar aplicativos, encaminhar um E-mail para um amigo ou ate mesmos quando efetuamos alguma ligação ou enviamos uma SMS. "Esses novos tipos de comunicação antes privados, agora são interceptados em massa pelo governo ou pelo setor privado onde quer que ele esteja" (ASSANGE, 2013, p43). Com o advento do mundo digital, as pessoas passaram a divulgam suas idéias e opiniões, posição políticas, laços familiares, fraternos e amorosos em mídias sociais como *facebook*, *twitter* ou *fousquer*. E a cada dia novas formas de comunicar ou gerar essas informações e metadados, são disponibilizadas para facilitar a vida de todos, a exemplo

das IOT (internet das coisas) que visa conectar objetos que ainda estão desconectados. Isso tudo mesmo já possuindo muitos *gadgets* conectados como os celulares, computadores, câmeras, óculos, TV, Impressoras e GPS.

Se por um lado toda essa disponibilidade de comunicação facilita a vida a cada momento, esse "estar conectado" cobra e cobre mais tempo, informação, dados e invadem a privacidade das pessoas sem necessariamente elas se darem conta. Internet, GPS, cartão de credito, mídias sociais, E-mail e celulares entre tantas outras "coisas eletrônicas" que já utilizamos, estão se tornando fontes de alimentação para a criação de verdadeiros perfis econômicos, sociais e culturais que são utilizados por governos e empresas para vigiar, controlar e lucrar.

A tendência é que o numero de chips por pessoas cresça e os RFID (dispositivos de radio frequência) estarão presentes em todos os lugares gerando cada vez mais informações sobre quase tudo que diga respeito ao cotidiano das pessoas, ou seja, a saúde, educação, esportes, transportes e alimentação, proporcionando assim um ambiente cada vez mais totalizador. Para os *cyberphunks*, essa será a real experiência do *panóptico*, prisão concebida pelo filósofo inglês Jeremy Bentham em 1787, da qual um único guarda poderia vigiar todos os prisioneiros ao mesmo tempo através de uma única linha de visão.

Num outro trecho do "Manifesto de um Cypherpunk", Hughes (1993) exemplifica essa relação entre esses novos modelos de comunicação e a perda da privacidade. Além disso, o autor demonstra como deveria ser a relação entre os participantes de um dialogo ou de uma transação, evitando assim essa experiência *panóptica* presente no cotiando:

> Quando compramos uma revista em uma loja com dinheiro, não há necessidade de saber quem eu sou. Quando eu pedir ao meu provedor de correio eletrônico para enviar e receber mensagens, o meu provedor não precisa saber com quem estou falando ou o que estou dizendo ou o que os outros estão dizendo a mim, meu fornecedor só precisa saber como passar a mensagem e quanto devo em taxas. Quando a minha identidade é revelada pelo mecanismo subjacente à operação, não oferece privacidade (HUGHES, 1993).

Em outras palavras, não podemos nos revelar seletivamente, devemos *sempre* nos revelar. Para os *Cypherpunk*, essa é a lógica atual dentro do Ciberespaço: uma forma de vida orwelliana, que está cada vez mais presente com desenvolvimento da informação e com uma tendência advinda de uma sociedade movida pelo informacentrismo.

O principal objetivo do movimento Cypherpunk vem da máxima "Privacidade para os fracos, transparência para os poderosos", ou seja, devolver ao indivíduo o controle sobre a sua comunicação e liberdade em ambientes de rede. Difundindo a utilização de criptografia para

alcançar à liberdade e combater a vigilância. Grupos de ativistas digitais desafiam governos em uma batalha que esta escrevendo o futuro da internet. Corporações, empresas e principalmente os governos espionam tudo que estamos fazendo em rede uma constante vigilância dos nossos dados armazenados em servidores espalhados por todo mundo.

Todavia, é importante citar que uma das principais característica presentes nesses meios de comunicações é justamente a da ubiqüidade, descentralidade, não-horizontalidade e velocidade. Afinal, os meios de comunicação digital têm a capacidade de transformar *átomos* em *bits* (NEGROPONTE, 1995). Nesse sentido, o que é **v**isto de forma ameaçadora pelos governos pelo fato de proporcionar um ambiente descentralizado de poder e informação, que auxilia o ativismo na rua e em rede, ajudando assim na divulgação dessas idéias. Em suma, o mundo do ciberespaço pode ser utilizado tanto para limitar nossa privacidade quanto para burlar a imposição dos meios de comunicação de massa que verticalizam a informação.

CIBERESPAÇO E O ATIVISMO DE SOFÁ

Expressados pelo *Slacktivism*, o ciberativismo, ou simplesmente ativismo de sofá, é um termo que, de acordo com a UNAIDS (Programa Conjunto das Nações Unidas sobre HIV/Aids), diz respeito a "pessoas que participam de uma causa fazendo o mínimo possível de esforço e que não estão realmente engajadas numa mudança de verdade". Nesse sentido, o ciberespaço possibilitaria, em tese, que os esforços das pessoas nas mais diversas manifestações eram mínimas, uma vez que poucas pessoas tinham acesso ao mundo virtual e não era atribuída muita importância ao ciberespaço. Todavia, esse conceito de que o ciberatismos não é importante esta mudando.

Hoje, não limitado apenas aos cliques, os ativistas digitais saem às ruas tornando-se ativistas do real. É difícil pensar quem hoje não esteja conectado. De certa forma, é possível perceber como num país como o Brasil, por exemplo, boa parte da população vem sendo atingida por essa onda ciberativista. Um exemplo preciso é o do movimento dos *Black Blocs*, que utiliza vandalismo como forma de protesto na pagina Black Blocs SP Fase II (pagina no facebook[6]). Cada vez mais eles divulgam para seus seguidores e adeptos um manual de como devem agir para não serem encontrados pela policia civil. No tutorial, eles incluem como navegar anonimamente, enviar mensagens sem deixar rastros e criptografia de arquivos.

É nesse contexto que o mundo *real* e *virtual* se misturam, distintos materialmente, eles acabam se encontrando pela proximidade criada pela cibercultura – expressão que diz respeito

[6] https://www.facebook.com/BlackBlocSPFaseII.

a todas as culturas, proporcionada pelo encontro de todos os povos que habitam esse terreno e através dele tem pautado, dominado e reconquistado o mundo real através da mobilização, ações e protestos na *ágora* virtual e nas ruas. Aqui, é importante não confundir *virtual* com *irreal*. Na reflexão filosófica, por exemplo, o virtual é um aspecto da realidade, mas que existe em potência, não em ato. Todavia, ainda assim o virtual é uma dimensão importante da realidade. Aqui, o conceito de *real* não necessariamente é sinônimo de algo tangível, material. Nesse sentido, Pierre Levy (1999, p. 49) afirma que "é virtual toda entidade 'desterritorializada', capaz de gerar diversas manifestações concretas em diferentes momentos e locais determinados, sem contudo estar ela mesma presa a um lugar ou tempo particular"[7].

Assim, dessa proximidade entre esses dois "mundos", virtual possa a ser "confundido" com o real ao ponto de ações que são praticados em espaços físicos tomem formas digitais de existir. Uma passeata ate a um determinado órgão publico, parando o transito, é mesmo que todos os ativistas entrando no site governamental dificultando o acesso, abaixo assinados, petições e atos de vandalismo. Ou seja, o mesmo que ocorre no mundo real existe no virtual. Dessa forma, sites costumam ser invadidos, pichados, alterados ou removidos por *hackers*. Estas são características do ciberativismo que geralmente tem um cunho político, ambiental e social, realizados através desses novos meios de comunicação digitas e do conhecimento crescente da programação.

A visibilidade e a importância que esta sendo atribuída a essa forma de protesto na rede de computadores tem mudado a forma de ver o ativismo digital. A cada dia as ações em rede tem se tornado uma ferramenta pessoal e coletiva de modificar o cotidiano assim como foi revolucionário a reprodução da escrita com a invenção da prensa mecânica. Antes da web o individuo consumidor, eleitor, cidadão ou telespectador só poderia comentar entre seus grupos e tribos sua insatisfação ou opinião. Pouco podia fazer para mudar uma situação. Hoje ele continua a comentar, só que agora em rede. Com isso, ele adquire o poder de produzir e divulgar com a democratização possibilitada pela hipermídia e as NTIC (Novas Tecnologias da Informação e Comunicação).

Assim, governos e empresas passam a olha e ouvir o que as pessoas pensam e dizem - principalmente no âmbito público – o que elas compartilham e curtem a seu respeito. Os governos estão interessados em saber como andam sua reputação, principalmente com o surgimento dessas novas formas de política que vem se construindo a partir da rede, a

[7] Um exemplo útil para entender essa diferença é a *palavra*: o termo *televisão* ou *árvore* remetem a objetos conhecidos pelo ser humano, mesmo que eles si mesmo não tenha uma realidade concreta, presas a um tempo e a um espaço particular. Todavia, a palavra televisão existe realmente, mesmo que não tenha sua coordenada no espaço tempo localizada graças a sua imaterialdade (LEVY, 1999).

exemplo dos Partidos Piratas. O que antes era um "ativismo desconectado", com os meios de comunicação de massa, na web 1.0 se torna uma grande voz na era pos-massiva da web 2.0. Seu poder de organização e difusão foram ampliados foi dado as massas um alto-falante global e universal.

OS CIBERPHUNKS E A MILITARIZAÇÃO DO CIBERESPAÇO

Talvez sejam esses os motivos que levam os estados a vigiar tudo e todos. É o que podemos chamar de "militarização do ciberespaço": não é mais suficiente tentear controlar os indivíduos na rua ou nos tradicionais meios de comunicação, pois eles encontraram uma nova praça. Pouco a pouco esse novo espaço se torna cada vez mais ocupada militarmente.

E ai que podemos observar a semelhança entre o mundo real e o virtual. Quando nos movimentamos entregamos nossa localização através de dispositivos móveis ou somos acompanhados por câmeras espalhadas por toda parte. Isso sem desconectar um instante do ciberespaço, entregamos não só o que fazemos, mas também o que pensamos mesmo distante dos olhos das câmeras. O nosso Storybord diário continua a ser desenhando por nós mesmo ao entregar tudo através do facebook, foursquare, instagran e Google. Basicamente como fala o autor no livro sobre o processo de vigilância:

> É como ter um tanque de guerra dentro do quarto. É como ter um soldado entre você e a sua mulher enquanto vocês estão trocando mensagens de texto. Todos nós vivemos sob uma lei marcial no que diz respeito às nossas comunicações, só não conseguimos enxergar os tanques – mas eles estão lá. Nesse sentido, a internet, que deveria ser um espaço civil, se transformou em um espaço militarizado. Mas ela é um espaço nosso, porque todos nós a utilizamos para nos comunicar uns com os outros, com nossa família, com o núcleo mais íntimo de nossa vida privada. Então, na prática, nossa vida privada entrou em uma zona militarizada. É como ter um soldado embaixo da cama. É uma militarização da vida civil". (ASSANGE, 2013.p.53)

Para os *Cyberphunks*, a intenção das empresas e governos é essa, ou seja, a de criar postos de vigilância por todas as partes. Câmeras por todo lado, bancos conectados a internet, sistemas de saneamento básico controlado por computadores, em suma, tudo tende a depender de um controle central que geralmente esta nas mãos do estado ou que pode ser acessado por ele. Contra isso, os grupos defendem o uso de criptografia e a utilização de sistemas anônimos, Software livre, e o uso de navegadores como o *Tor* que desempenha um papel fundamenta na privacidade dos usuários da rede. O que deixa muitos governos sem saber como reagir diante dessa "ameaça" que é a internet, seu poder de concentrar informação e conectar as pessoas promovendo verdadeiras revoluções a partir dos hipertextos, blogs, sites de vídeo ou redes sócias. A única forma encontrada pelo estado para "controlar" e fiscalizar a

internet é através da utilização de software sobre a seguinte idéia: "Precisamos nos imunizar caso isso afete o nosso pais, caso esse negócio de internet chegue aqui. Precisamos controlar isso completamente, precisamos filtrar, precisamos saber tudo o que eles estão fazendo" (ASSANGE, 2013.p.44).

O que fez o regime de Ben Ali, um dos mais corruptos e com maior taxa de desemprego, por exemplo, mantinha filtros a vários sites principalmente ao de compartilhamento de vídeo que foram banidos ate a queda do ditador, que não contava com o poder das mídias sócias Twitter, Facebook e Youtube principalmente do Facebook que continuou ativo na rede mundial. Com a censura estatal as mídias, Tevê, Jornais e Rádio sobre o comando do regime, os revoltos só puderam contar com as redes telemáticas de (telefonia, satélite, cabo, fibras ópticas), e as mídias sociais como as únicas formas de comunicação, logo todo cidadão passou a atuar com repórter registrando a partir das câmeras de celulares os conflitos e testemunhos.

Antes da queda do regime os internautas, ao tentar acessar alguns sites não permitidos pelo governo, se deparavam com a pagina de erro 404 apelidada de "Ammar 404". A Organização RSF (Repórteres Sem Fronteiras) removeu o pais da lista de "inimigos da internet" para a lista "sob vigilância" logo a pois a entrada de um novo governo provisório.

A internet não foi nem será a causa dos protestos ou revoltas, mas é sem sombra de duvidas um grande oráculo a serviço da sociedade na organização e divulgação dos movimentos. Um professor da cidade de Tala, explica o que as pessoas estavam fazendo para disseminar a notícias nesse novo cenário pos-midiatico: "Faço fotos dos protestos nas ruas, anoto declarações de testemunhos e coloco tudo no Facebook". Além disso, conta Sayhi, ele e seus colegas de protesto mantêm estreito contato com agências internacionais de notícias. (DW.DE.COM).

Assim como foi no Brasil no ano de 2013: esses novos meios de comunicação pos-massivos funcionaram como extensões (MCLUHAN, 2007) dos corpos, da voz e da presença humana, que agora não mais pertence ou aplica-se a um único indivíduo como era na era nos meios de comunicação de massa, mas é composto por uma teia de idéias em parte homogêneas, que ganham formas a partir dos vídeos, imagens, *podcasts, software livres* ou *pee to peer* tudo potencializado pelo tripé da Cibercultura: emissão, conexão e reconfiguração (LEMOS,)[8].

O regime de ben Ali censurava a internet com a utilização do softwares SmartFilte, de

[8] http://www.hrenatoh.net/curso/textos/andrelemos_remix.pdf

fabricação americana, esse e outros programas são utilizados para bloquear, vigiar e encontrar terroristas entre os milhares de e-mails. Os programas de vigilância utilizados para monitorar o que se passa na comunicação são cada vez mais avançados e rápidos na detecção de possíveis ameaças de ataques terrorista. Porem nem toda essa qualidade e velocidade pode garantir a prevenção de algum ataque como o que aconteceu durante a maratona no ano de 2012, em Boston. E nem sempre a confirmação de um suposto terrorista é certa.

Isso se deve a falta de informações que possam formar um perfil mais claro dos que estão planejando um ataque. O software PRISM atua da seguinte forma: para realizar o trabalho de encontrar e cruzar dados o programa filtra rapidamente um banco de dados com milhões de E-mail em busca de uma combinação de palavras suspeitas, quando o algoritmo encontra algo uma pessoa ou o programa de computador analisa o conteúdo.

Apos detectar uma suposta ameaça os informações do suspeito é cruzada ate chegar a um perfil mais claro. Números vão sendo atribuídos a características da pessoa como: frequência com que viajou nos últimos anos, com quem se comunicou, por quanto tempo, de qual país, trabalha, tem cartão de credito, se é estrangeiro, etc. Essas informações geram uma sequência numérica atribuída aos suspeitos e comparadas a uma sequência numérica de outro terrorista. Quanto mais semelhantes às sequencia, maiores a as chances de se impedir um novo atentado. O problema é que pessoas comuns são identificadas como terroristas e o resto do mundo é vigiado.

E para manter a qualidade da defesa e monitoramento do pais os Estados Unidos a fim de qualificar as futuras gerações para essa nova forma de controle, segurança e vigilancia civil a Marinha Norte Americana organiza e patrocina Campeonatos como os que acontecem na Collegiate Cyber Defense, da universidade de Washington, os jovens são convidados a participar de um campeonato de defesa virtual. Porem o que esses jovens Ciberguerreiros tem que fazer não passa de um ciberataque entre os grupos que compõe o campeonato, a intenção é justamente formar os futuros guerreiros que custaram bem menos que uma aeronave não tripulável. O que deveria ser uma experiência de ciberdefensores é na verdade um campeonato hacker ofensivo. Acompanhado por funcionários da Cia que recrutam jovens patriotas que queiram defender o país.

Esse interesse na vigilância por parte do estado é realmente ameaçador e põe em risco o funcionamento da democracia, porem há também uma vigilância privada e a coleta de dados por grandes empresas do setor privado como os gigantes Google, Facebook ou Microsoft. O buscador mais famoso do mundo, por exemplo, sabe com quem nos comunicamos nossas redes de amigos, sua preferência sexual e religião. “eles sabem mais sobre você do que você

mesmo". (ASSANGE, 2013)

O problema do setor privado é que a cada dia o abismo das relações com o estado estão diminuindo, seja acordo, ou seja por intermédio da justiça. Apos a aparição do Edward Snoldem, ficou claro que grandes empresas passam informações dos clientesparao governo obrigados pela justiça. Mas, nada os impedem de negociar ou vender esses dados além do mais eles são "indústrias da informação" e sues melhores funcionários somos nós.

As agencias de espionagem dos Estados Unidos tem acesso a todos os dados do Google e do Facebook como ficou claro pelas declarações e documentos de *Snoldem*. Assim o setor privado é uma extensão das agencia de espionagem. Tentáculos amputados, mas conectados ao governo.

FORMAS DE PROTEÇÃO CONTRA ESPIONAGEM

Então como podemos fugir dessa constate ligação que mantemos com ambos os setores públicos e privados? Há quem sugira que apenas a desconexão seria a solução. Todavia, a utilização de métodos e ferramentas pode ajudar muito a minimizar essas praticas. E algumas formas de combater a vigilância é através de serviços de descentralização, hospedagem individual de dados e criptografia. Além da utilização de software livre como O navegador TOR (O roteador cebola) é um software gratuito que ativa o anonimato online. A rede Tor é uma rede de túneis http (com tls) sobrejacente à Internet, onde os roteadores da rede são computadores de usuários comuns rodando um programa e com acesso *web*. O objetivo principal do projeto é garantir o anonimato do usuário que está acessando a *web*. ferramenta usada nos vazamentos do Wikileaks e do ex-agente da NSA Edward Snowden.

Outras formas de proteção contra a vigilância são HTTPS EVERYWHERE extensão para Firefox e Chrome que oferece navegação mais segura: sempre que possível, direciona o navegador para conexões encriptadas do site que está acessando.PGP (Preety Good Privacy) é um sistema de criptografia que protege e-mails, arquivos (em discos rígidos ou na nuvem) ou computadores inteiros.COLLUSION extensão para Firefox que permite descobrir que sites estão rastreando sua navegação sem sua autorização.DUCKDUCKGO alternativa ao Google que permite pesquisas anônimas, pois não monitora as buscas feitas pelo usuário. DIASPORA alternativa ao Facebook que busca proteger os dados pessoais de seus usuários. Os Cryptophone telefones com proteção a possíveis escutas e grampos no qual algoritmos criptografam os sinais.

"Acho que precisamos desenvolver ambas paralelamente. Precisamos de um software

> livre que todo mundo possa entender, que todo mundo possa modificar e que todo mundo possa examinar para verificar o que ele está fazendo. Acho que o software livre constitui uma das bases para uma sociedade on-line livre, para termos o potencial de sempre controlar a máquina, não permitindo que ela nos controle. Precisamos de uma criptografia robusta para nos certificar de que ninguém mais possa ter acesso a dados que desejamos manter privados. Precisamos de ferramentas de comunicação como o Tor ou como o Cryptophone para ser possível nos comunicar só com as pessoas com as quais queremos nos comunicar." (ASSANGE, 2013).

Hoje, compondo verdadeiras redes, cidades, comunidades virtuais e grupos como o Wikileaks, Partido Pirata e Anonimos forma tribos de ciberativistas que querem divulgar suas pautas, opiniões ou discutir politica, cultura, meio ambiente e privacidade e contam com a criptografia para difundindo conhecimento sobre a liberdade de expressão, vigilância, meio ambiente

CONSIDERAÇÕS FINAIS

Como vimos, a rede mundial de computadores tem uma vertente dupla: o mundo do ciberespaço pode ser utilizado tanto para limitar nossa privacidade quanto para burlar a imposição dos meios de comunicação de massa que verticalizam a informação. Eles podem impulsionar os indivíduos para protestar contra formas opressivas de governo, ao mesmo tempo que podem servir para os mais diversos fins totalitários.

O movimento *Cypherpunks* surge em rebelião contra a perda de privicidade, cada vez mais comum dentro do ciberespaço. O principal objetivo do movimento *Cypherpunk* vem da máxima "Privacidade para os fracos, transparência para os poderosos", ou seja, devolver ao indivíduo o controle sobre a sua comunicação e liberdade em ambientes de rede. Para isso, o movimento lança mão da criptografia quando acessa uma rede de computadores a fim de terem a privacidade protegida. Os *Cypherpunks* acreditam que criptografia de forte algoritmo irá capacitar os indivíduos a se comunicarem com segurança e liberdade. Por isso, eles se opõem a qualquer tipo de regulamentação governamental da criptografia. Assim, grupos de ativistas digitais desafiam governos em uma batalha que esta escrevendo o futuro da internet.

REFERÊNCIAS

CYPHERPUNK. In: **OXFORD DICTIONARIES**. Oxford: Oxford University Press, 2014. Disponível em: <http://www.oxforddictionaries.com/us/definition/american_english/cypherpunk?q=Cypherpunk>. Acesso em: 27 mar. 2014.

CYPHERPUNK. In: **WIKIPÉDIA**, a enciclopédia livre. Flórida: Wikimedia Foundation, 2013. Disponível em: <http://en.wikipedia.org/wiki/Cypherpunk>. Acesso em: 31 mar. 2014a.

CYBERPUNK. In: **WIKIPÉDIA**, a enciclopédia livre. Flórida: Wikimedia Foundation, 2013. Disponível em: <http://en.wikipedia.org/wiki/Cyberpunk>. Acesso em: 31 mar. 2014b.

CYPHERPUNK. In: **Whatis.com**. Grove Street: SearchSecurity.com, 2014. Disponível em: <http://searchsecurity.techtarget.com/definition/cypherpunk>. Acesso em: 31 mar. 2014.

DERTOUZOS, Michael. **O que será**: como o novo mundo da informação transformará nossas vidas. São Paulo: Companhia das Letras, 1997.

HUGHES, Eric. **A Cypherpunk's Manifesto**. Berkeley, 1993. Disponível em: <http://www.activism.net/cypherpunk/manifesto.html>. Acesso em: 31 mar. 2014.

LEVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999.

NEGROPONTE, Nicholas. **Vida Digital**. São Paulo: Companhia das Letras, 1995.

THOMPSON, John B. **A mídia e a modernidade.** Petrópolis: Vozes, 2009.

ASSANGE, Julian e col: CYPHERPUNKS: Liberdade e o futuro da internet.

LEMOS, Andre. CIBER-CULTURA-REMIX¹. Disponível em: <http://www.hrenatoh.net/curso/textos/andrelemos_remix.pdf> Acesso em: 29 de mar de 2014.

AYARI, Chamselassil e col. **Censura reforça papel de redes sociais nos protestos na Tunísia e Argélia.** Disponível em: <http://www.dw.de/censura-refor%C3%A7a-papel-de-redes-sociais-nos-protestos-na-tun%C3%ADsia-e-arg%C3%A9lia/a-14762568-1>. Acesso em: 12 de mar. 2014.

HIPERMÍDIA e transmídia, as linguagens do nosso tempo -- Profa. Dra. Lúcia Santaella (PUC/SP). Conferência proferida pela Profa. Dra. Lúcia Santaella. Disponível em: <https://www.youtube.com/watch?v=vzlhvVHLE1s >. Acesso em: 22 de mar de 2014.