Quem Possui o Ciberespaço?

> *Quando você pisa no ciberespaço, você está em território de outra pessoa. Você anda nu diante de seu olho, que tudo vê. Sobre ele você não tem nenhum poder. Até os seus segredos internos - se você for estúpido o suficiente, para colocá-los no disco rígido do seu computador pessoal - estão abertos para o seu olhar.*

Para mim, a palavra "ciberespaço" tem uma etimologia duvidosa. É uma forma abreviada da palavra "cibernética", concatenado com a palavra "espaço". A palavra "cibernética" é derivada de uma palavra grega que, dependendo de seu contexto, pode significar leme, timoneiro, piloto ou governador. A palavra refere-se a espaço como um meio multidimensional, através do qual entidades conscientes, como os humanos, podem se tornar conscientes de si e interagir com o outro. Por conseqüência, a palavra ciberespaço deve se referir a um meio multi-dimensional, que algumas entidades conscientes usam como um dispositivo de leme de direção ou por meio do qual governa ou controla o resto de nós. Para mim, isto está muito próximo da verdade.

O meio multi-dimensional do espaço cibernético deve, portanto, incluir, em primeiro lugar, a “terra-espaço” - a biosfera física do nosso planeta. Afinal de contas, o nosso principal meio de comunicação é para, através de viagem, conhecer e conversar com outras pessoas cara-a-cara. A biosfera é preenchida com ar, que conduz o som da voz humana. É, portanto, um meio através do qual os seres humanos podem conversar. Este meio é um canal ideal para a comunicação humana. Através dele, o discurso humano normal oferece um canal de comunicação, com uma largura de banda muito grande sobre uma distância convenientemente limitada. Isto facilita o rápido intercâmbio de conhecimentos, pensamentos e idéias com controle seguro e fácil entre a privacidade, de um lado e a publicidade, de outro lado.

Devendo ser incluído, também, o espaço do “rádio-espaço” - o que conhecemos como o espectro eletromagnético, que compreende toda a gama de ondas de rádio, através das quais somos capazes de comunicar a uma distância quase como se face-a-face. E, finalmente, é claro, que inclui a Internet. Pessoalmente, eu questiono se ou não estes avanços técnicos relativamente recentes, realmente oferecem qualquer vantagem para o bem-estar da humanidade. Minha percepção relutante é que a humanidade, ainda, tem, certamente, que ganhar a sabedoria necessária e suficiente, para usar tais avanços técnicos, de forma adequada e construtiva e não como um instrumento para o condicionamento, a tranqüilização e a exploração das populações crédulos.

O discurso que se segue é sobre todos esses três aspectos do ciberespaço e o que se passa dentro deles, conforme a minha percepção de onde eu estou dentro do tempo, do espaço e da ordem social.

Quem Possui a “Terra-espaço”?

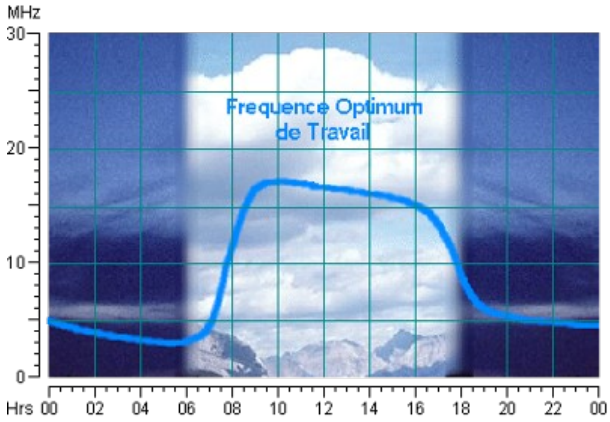
Talvez nos primórdios enevoadas da humanidade, as pessoas vagavam, sem obstáculos, por toda a superfície abundante de seu planeta natal, capaz de livremente comunicar-se e interagir com os seus pares. Mas não demorou muito para que os reis começassem a anexar terras habitáveis da Terra, e os recursos nele contidos, como um meio de regular e controlar a maioria da humanidade e, assim, comandar o seu trabalho. Hoje em dia, a única forma de o indivíduo se mover ao longo da superfície do nosso Planeta é através de uma infraestrutura de transportes, o que está longe de ser livre, e dentro da qual, os movimentos dos

indivíduos são severamente restringidos, regrados e controlados. A Terra não é mais livre para nela passearmos.

Hoje, as pessoas podem se comunicar e interagir em toda a superfície física do Planeta, mas apenas com a permissão de seu Estado e dos proprietários das terras. E estes exigem o pagamento para a concessão de sua licença. Eles, também, impõem regras restritivas acerca de que rotas o indivíduo pode usar, além de como, quando e em que condições ele pode usá-las. Eles controlam toda a terra. Controle é da propriedade. Mesmo nas economias prósperas do Primeiro Mundo, o indivíduo não tem direito absoluto sobre qualquer pedaço de terra neste Planeta. Ele ainda tem que pagar pelo "privilégio de possuir a sua moradia", ainda que no subúrbio.

Na minha opinião, este não é um estado idílico para a espécie humana. Cada indivíduo é um ser consciente independente. Coletivamente, a humanidade não é uma entidade consciente. Nem é uma família, um Estado ou uma corporação. Estes não têm medo ou sentimento pessoal. Por isso, é o bem-estar de cada indivíduo consciente que importa. Cada indivíduo deve, portanto, com razão, ter livre e desembaraçado o uso econômico de seu quinhão de terra-espaço e o direito de passagem livre por toda a terra-espaço, com sentido de que este indivíduo não deve perturbar o uso econômico de outros possuidores de terras. Nenhuma coletividade tem poder moral para tirar esses direitos do indivíduo.

Quem Possui o Rádio-Espaço?



Em 1867, James Clark Maxwell fez sua previsão matemática da existência das ondas de rádio. Dois anos mais tarde, Heinrich Hertz conseguiu gerá-las artificialmente. Experiências que se seguiram revelaram que estas ondas podem ser feitas para saltar entre o chão e as camadas ionosféricas e, assim, propagam-se por todo o globo terrestre. Antes desses eventos, nada se sabia sobre essas ondas ou sobre as dimensões do espaço-tempo através do qual elas viajam. E o que é desconhecido não pode ser comandado nem por reis nem por corporações. Consequentemente, antes de sua descoberta, o espectro de rádio era uma terra virgem intocada, selvagem, não reclamada e livre. Qualquer um poderia construir seu próprio aparelho e experimentar conforme determinasse o seu coração.

Mas não por muito tempo. Tal como aconteceu com os continentes livres do Novo Mundo, reis, imperadores, empresas e corporações logo olharam para o espectro das ondas do rádio com olhos possessivos. Cada um reuniu o seu poder de dividir e conquistar para obter ganhos lucrativos. Cada um dos reis da Terra logo declarou sua posse dentro de sua respectiva jurisdição das dimensões recém-descobertas do espaço-tempo, através do qual viaja a onda eletromagnética. O homem comum não podia mais se aventurar nele, a não ser com a permissão de seu rei.

Para cada governo, o rádio-espaço é de valor inestimável para a administração, defesa e como uma fonte de receita comum. Assim, hoje, cada Estado reserva para si alguma porção do espectro de rádio, para uso de suas forças armadas e dos serviços públicos. Ele concede licença de uso do que resta para seus súditos e governados, em troca de uma taxa. Ele licencia algumas delas para emissoras de TV, algumas para a marinha-mercante, outras para os operadores de aeronaves, e, também, para algumas operadoras de comunicações comerciais ou de comunicações privadas, e, até mesmo, para alguns entusiastas de radioamador.

Como sempre, quando um rei concede sua licença, ele vem com termos e condições. No caso da licença de utilização do espectro de radiofrequências, ele vem com termos e condições muito restritivas. A licença do titular é restrita, não só quanto ao trecho de freqüências e potência que ele pode usar, mas, também, quanto ao tipo de informação que ele pode enviar e receber.

As restrições impostas aos radioamadores são extremamente restritas. Comentários e discussões políticas, religiosas e comerciais são expressamente proibidas. É provavelmente inseguro, até mesmo, para discutir filosofia. Na verdade, os únicos temas, que os radioamadores podem seguramente discutir, são sobre os seus equipamentos, as condições meteorológicas e as condições de sinal. Isso faz com que as conversas sejam tediosas.

Rádio-espaço está, portanto, absolutamente fora dos limites para qualquer indivíduo que queira discutir livremente as suas próprias ideias e opiniões políticas, religiosas, filosóficas ou comerciais com outras pessoas. Às vezes, em vão, eu tento imaginar o que seria se eu fosse membro de um fictício grupo igualitário, em que somente os seus membros conhecessem sobre a existência das ondas de rádio e como usá-las na comunicação. Teríamos liberdade plena, sem ônus econômico para discutirmos tudo o que gostássemos, sem impedimentos por quaisquer restrições e regulamentações impostas pelo rei ou pelo Estado. Mesmo que nós tivéssemos descoberto uma técnica secreta, como a transmissão digital de espalhamento-espectral-fatiado na década de 1950, poderíamos ter comunicado por rádio entre nós, porque nenhuma autoridade da época não teria consciência dos nossos sinais.

Nenhum Estado quer que os indivíduos tenham liberdade sem licença e sem censura para discutir todos e quaisquer assuntos com qualquer outro indivíduo dentro de sua jurisdição. Se pudessem, diferentes pessoas de diferentes áreas de conhecimento e crenças poderiam se conectar livremente. Conectados eles se uniriam. Unidos eles não poderiam ser divididos. União que não poderia ser descartada. E isto seria uma ameaça real e presente para o poder governamental.

Ao contrário da terra-espaço, o rádio-espaço é tridimensional e não se limita à superfície da Terra. Ele ocupa todo o universo. Então, até que ponto pode um Estado soberano reivindicar isso? Ele não pode ser vedada como a terra. Um Estado não pode parar as ondas de rádio de cruzar suas fronteiras nacionais. A única medida em que um Estado pode reivindicar a posse do rádio-espaço é controlar o seu uso por seus súditos ou governados. A única maneira de fazer isso é através da imposição de uma penalidade da lei ao indivíduo, que usa rádio-espaço dentro de seus limites territoriais, sem licença ou de um modo ou para uma finalidade que a lei proíbe. O Estado policia seu rádio-espaço, para ver quem pode estar violando esse aspecto de seu "território soberano", simplesmente por meio do monitoramento do espectro de rádio das estações oficiais de escuta.

Tendo imposto um rigoroso controle sobre quem pode ou não pode transmitir sinais de dentro de seus respectivos territórios, alguns estados soberanos proíbem seus súditos ou governados, até mesmo, de receber passivamente os sinais de rádio, sem que tenham que pagar uma taxa de licença. Isto foi abolida no Reino Unido em 1971, mas esta exigência legal ainda continua para a recepção de programas de televisão.

O dinheiro da taxa de licença é supostamente utilizado para a criação de programas e execução dos serviços de transmissão. Não obstante, ele coloca a autoridade de radiodifusão do Estado na posição de receber financiamento incondicional, para produzir o que a autoridade quer que as pessoas vejam e ouçam, o que não é, necessariamente, o que as pessoas querem ver ou ouvir. Mais preocupante, cria-se um mecanismo, pelo qual o Estado e sua autoridade de radiodifusão podem orientar e manipular a opinião pública, tornando-se um meio eficaz de controle da sociedade, em conformidade com a vontade do Estado e da elite minoritária, que realmente influencia e controla.

Um Estado soberano não pode parar a entrada das ondas de rádio de outros estados soberanos no seu território. Nem pode parar as ondas de rádio, que emanam de dentro de sua jurisdição de sair e entrar nos territórios de outros Estados soberanos. Um determinado estado pode querer impedir que os estrangeiros ouçam as suas transmissões domésticas. Ele pode tentar fazer isso, limitando a potência e/ou utilizando bandas de frequência de linha de limite da visão. O mais provável, porém, pode querer impedir que os seus súditos recebam transmissões de alguns Estados estrangeiros, por razões de políticas conflitantes. Isto pode ser conseguido através da transmissão de sinais de interferência na mesma freqüência que a transmissão ofensiva, como aconteceu durante a Guerra Fria. Hoje em dia, com a transmissão digital, o controle completo de quem pode ou não receber uma transmissão pode ser efetuado por incripção do sinal.

Então, depois de ser descoberto, como deve a humanidade usar o rádio-espaço? A resposta, na minha opinião, deve ser usado de uma maneira, que seja mais justo para todos os indivíduos. Cada indivíduo, caso queira, deve ser livre para usar o rádio-espaço e, através dele, procurar e encontrar pessoas com os mesmos ideais e discuti-los aberta e livremente com elas. Ele, também, deve ser livre para difundir suas idéias com qualquer pessoa, que queira ouvi-las. Ele, também, deve ser livre para contatar alguém, seja casualmente ou por algum motivo específico. Da mesma forma, ele deve ter assegurado o direito à privacidade de não ser incomodado por chamadas persistentes, como a epidemia atual e indesejável dos call centers de televendas.

Existe tecnologia em que tudo isso poderia ser facilmente implementado, sem infraestrutura comum. No entanto, para que ele funcione de forma equitativa, deve haver alguma forma de coordenação central. Uma entidade singular deve existir para gerenciar o espectro, alocando canais para sessões e mantendo os índices de busca. Mas uma tal entidade não deve ser autoridade com força coercitiva. Também, nunca deve ser permitido cair nas mãos de quaisquer interesses privados, sejam comerciais ou não. Deve ser um sistema passivo, implementado como uma tecnologia distribuída dentro dos equipamentos de todos os seus usuários.

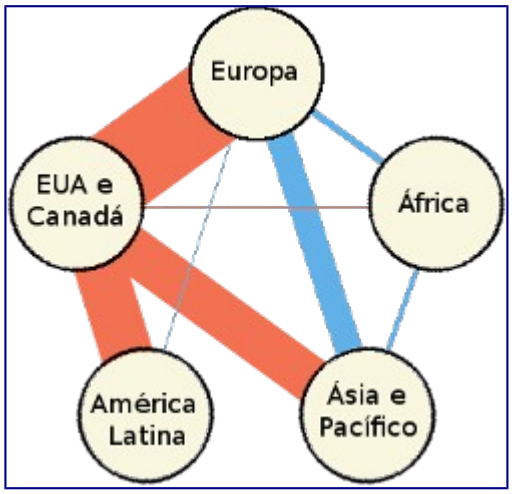
Quem é Dono da Internet?

Rádio-espaço é um aspecto do universo natural. A Internet não é. Dois radioamadores, em diferentes partes do mundo, podem se comunicar uns com os outros através de rádio HF, usando transceptores projetados, construídos e pertencentes inteiramente por si mesmos. Neste caso, os dois emissores-receptores estão ligados por meios totalmente naturais. Dois *geeks*, em diferentes partes do mundo podem se comunicar uns com os outros, através da Internet, usando computadores pessoais projetados, construídos e de propriedade inteiramente por eles mesmos. Neste caso, no entanto, o que conecta os dois computadores pessoais é uma infraestrutura artificial muito complicada e cara.

A justificativa para o custo extremo de infraestrutura da Internet é que o rádio-espaço simplesmente não tem a capacidade de transferência de dados em velocidades exigidas por todos os usuários da Internet. Pelo menos, não na forma como a Internet é implementada atualmente. E a forma como a Internet é implementada tem muito a ver com a forma como ela nasceu, desenvolveu-se e evoluiu.

Uma parte do que se tornou a Internet, a *Joint Academic Network*, começou a partir do desejo de cientistas e acadêmicos, em centros de pesquisa e universidades de todo o mundo, de trocar rapidamente artigos científicos e dados experimentais. Eles optaram pela solução rápida de alugar o uso de cabos ou serviços de pacotes de autoridades e empresas nacionais de telecomunicações. Outras redes, que se tornaram parte da Internet, começaram como redes de ligação de centros governamentais em vários países, novamente usando cabos alugados. Ainda outras redes, que se tornaram parte da Internet, começaram como redes privadas, operadas por grandes transnacionais, através de cabos alugados. Essas três partes e todos os seus vários elementos, finalmente, por mútuo acordo, tornaram-se interligadas para formar as redes interconectadas ou Internet.

Consequentemente, os cabos de ligação são de propriedade de telefônicas dos estados ou são de corporações licenciadas pelo estado, cada uma operando dentro de sua jurisdição geográfica designada, em todo o mundo. As empresas de telecomunicações podem também possuir os nós de comutação (ou roteadores), nos vários cruzamentos das rotas de cabos. Equipamento para comutar (ou roteamento) pode, no entanto, também, ser de propriedade de empresas privadas, que alugam o uso dos cabos que conectam os nós de comutação privada. Todos estes juntos formam o que é chamado de "coluna" (*Backbone*) da Internet, que se estende por todo o globo.



Uma visão geral lógica da estrutura global está indicada à esquerda. A largura de cada linha vermelha representa a quantidade relativa de tráfego de dados, que passa entre cada par das cinco principais regiões do mundo. De longe, a rota mais movimentada é entre os EUA e a Europa. Praticamente, 100% do tráfego da América Latina, com destino ao resto do mundo, flui através dos EUA. A gritante omissão é uma rota que ligue a América Latina com a África. Com quase todo o tráfego de dados de todo o mundo fluindo através dos EUA, este país, efetivamente, é capaz de interceptar, monitorar, gravar, parar ou interromper todos os dados que fluem ao redor do mundo.

Todos os interesses privados que operam dentro dos EUA, incluindo todos os proprietários e operadores de cabos e roteadores de Internet, através do qual, praticamente, todo o tráfego de Internet do mundo passa, estão sujeitos à lei dos EUA. Consequentemente, o governo dos Estados Unidos da América - por meio de suas várias agências - é capaz de controlar o fluxo de tráfego dentro da infraestrutura física da Internet no mundo todo.

Um roteador de Internet fica em cada junção da Internet. Sua função é de transmitir a cada pacote de dados, que chega até a próxima etapa adequada de sua rota, para o seu destino final. Cada pacote de dados contém informações sobre os endereços de origem e de destino. A maioria dos roteadores estão localizados no território dos EUA e, portanto, sob a jurisdição da lei americana.

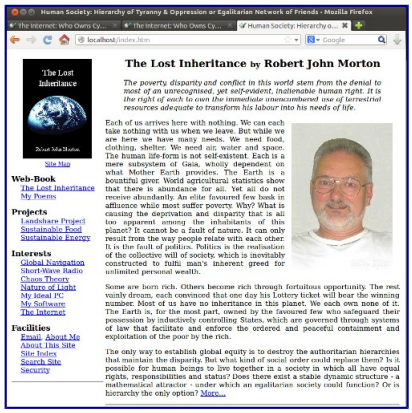
O governo dos EUA está, portanto, em posição de ser capaz de emitir um instrumento jurídico a um administrador de roteador, proibindo-o de enviar pacotes de dados que viajem entre uma determinada origem, (quer seja, dentro ou fora dos EUA) e um determinado destino (quer seja, dentro ou fora do EUA). Com o software adequado ou *firmware* de *chips* secretamente incorporado dentro de um roteador, uma agência do governo dos EUA poderia efetivar o bloqueio remotamente, sem que o administrador do roteador tivesse ciência disto.

Eu não estou sugerindo que eles fazem isto. Mas o ditado geral é que, se puderem, eles fazem. Eles são capazes, portanto, à própria vontade, de tornar visível ou invisível um *site* de um país estrangeiro em outros países.

Não obstante, a posse efetiva da infraestrutura física da Internet não importa no controle técnico sobre que tipo de informação ela carrega. A Internet está aberta internacionalmente e, portanto, o conteúdo semântico do tráfego de dados, que flui através dela, está fora do controle direto de qualquer estado soberano ou jurisdição legal. Para controlar verdadeiramente a Internet, é necessária a construção de alguns meios para controlar que tipo de conteúdo semântico pode passar através da Internet e quem pode ou não acessá-lo.

Por causa de sua posição central na infraestrutura mundial da Internet, os EUA, através da ação de encorajamento seletivo, consegue estabelecer múltiplos meios, para alcançar o controle total do conteúdo da Internet ou, pelo menos, controlar o acesso desse conteúdo pelo público mundial. Esses meios estão, para todos os efeitos práticos, exclusivamente, concentrados dentro da jurisdição dos Estados Unidos, onde, mais uma vez, eles podem ser regulados pela lei americana.

Controle da *Web* Mundial



Qualquer cientista ou acadêmico ou, na verdade, qualquer pessoa, que queira, pode publicar suas observações, experiências, sofrimentos e opiniões na rede mundial, como é o exemplo do meu próprio *site* mostrado à direita. Tudo que ele precisa fazer é escrever seus pensamentos em um arquivo de texto, marcá-lo em HTML [*hypertext markup language*] e fazer o *upload* para um servidor *Web*. Ele pode incluir, dentro de seu texto, diagramas, fotografias, animações e programas ainda em execução, chamado *applets*. Mas como é que as outras pessoas conseguem ver o que ele, assim, publicou?

HTML inclui um meio, na sua sintaxe, que contém uma lista de palavras-chave. Este meio é chamado a *keywords meta tag*. O autor do documento coloca as palavras-chave relevantes para a *keywords meta tag* de seu documento. Estas palavras-chave são as que o escritor do documento pensa ser a que, provavelmente, vêem à mente das pessoas, quando elas estão à procura de material sobre os temas ou ideias do seu artigo. As palavras que, realmente, surgem nas mentes das pessoas, quando elas estão pensando em um assunto ou ideia particular, não são necessariamente as que aparecem nos textos dos documentos mais relevantes. Portanto, escolher palavras-chave eficientes é, realmente, uma arte.

Alguns computadores, conectados à Internet, contêm programas em execução, chamados de *"search spider"* ou, em português, “busca da aranha”. Estes continuamente arrastam através de todos os documentos em todos os servidores na rede mundial de computadores. Cada “aranha” olha no *“key word meta tag”* de cada documento. Em seguida, este programa coloca as referências a esse documento com todas as palavras-chave relevantes em seu vasto índice de pesquisas.

Nesses mesmos computadores, também, opera um outro tipo de programa chamado de *search engine* ou motor de busca. Este é acessado através de uma página *Web*, a qual é mostrada à esquerda.

Uma pessoa, pesquisando determinados documentos sobre um tipo de assunto, digita as palavras-chave relevantes, que lhe vêm à mente, no campo de busca. A seguir, clica no botão "Ir". O *"search engine"*, então, pesquisa, em seu vasto índice, por documentos relevantes. Então, exibe uma lista de títulos dos documentos relevantes encontrados, juntamente, com um breve resumo abaixo de cada título. O pesquisador, então, clica no título que lhe interessa, para visualizar o documento no seu navegador.

Os *"search engines"* e suas *"spiders"* eram serviços auxiliares e gratuitos, operados dentro de grandes computadores de instituições acadêmicas e de outras organizações não comerciais.

Documentos eram listados, estritamente, de acordo com a relevância e nada mais. As pessoas podiam encontrar exatamente o que queriam dentro de tudo o que era disponível. "E todos viveram felizes para sempre". Ou seja, até que os negócios e o comércio colocaram suas mãos sujas e tortuosos na rede mundial, corrompendo todo o processo.

O motivo natural dos acadêmicos e dos outros pensadores era fazer com que o material estivesse disponível para as pessoas, que, genuinamente, fossem interessadas nas matérias disponibilizadas para pesquisas. Eles não tinham desejo de empurrar o seu material “goela abaixo” às pessoas que não tivessem interesse pelo material. Porém, esta não é a intenção do empresário. Ele quer atrair qualquer um e todos ao seu *site*, a fim de enganá-los, por todos os meios possíveis, para a compra de seus produtos. E ele, rapidamente, encontrou uma maneira eficaz de fazer isso.

O empresário compila uma lista de palavras de busca mais populares, que as pessoas utilizam nas suas pesquisas. Estas são, em sua maior parte, palavras com conotações sexuais, esportivas ou financeiras. Então, ele utiliza essas palavras - juntamente com palavras-chave que são relevantes para o seu próprio negócio – *keywords meta tag* na primeira página de seu *website*. Assim, não só as pessoas que procuram, especificamente, os seus produtos, mas, também, um grande número de outras pessoas, que estavam à procura de algo completamente diferente, acabam acessando a sua página. Sua esperança é que essas outras pessoas, tendo chegado em seu *site*, sejam seduzidas por sua apresentação atrativa para a compra de sua mercadoria.

A sobrecarga da *keywords meta tag* com falsas palavras atraentes, eventualmente, tornou-se um incômodo tão esmagador para os usuários da Internet, que os *search engines* tradicionais tornaram-se quase inúteis para pesquisas sérias. Algo drástico tinha que ser feito. A solução foi abandonar a *keywords meta tag*, como meio para as *search spiders* classificarem as páginas da *Web*. Os *search engines*, desde então, passou a ignorar o conteúdo da *keywords meta tag* completamente, ao invés de extrair as palavras-chave diretamente do texto do documento.

É claro que essa prática não se presta à compilação das palavras-chave mais eficazes. A maioria das palavras que as pessoas pensam, quando procuram por um documento, não são susceptíveis de aparecer como tal no texto do documento. Palavras-chave são, geralmente, palavras de sentido complexo e altamente específico. O pensamento contido na palavra-chave é normalmente expresso de modo muito mais poderosa dentro do texto real por uma frase, que compreende uma combinação sucinta de palavras mais comuns. Assim, o processo de busca já perdeu parte de sua eficácia original. Mas isso é apenas o começo dos problemas.

Para compensar este problema da menor eficácia na “colheita” de palavras-chave, os autores das páginas da *Web* começaram a escrever textos em que eles, deliberadamente, substituíram frases compostas de várias palavras simples por palavras mais eruditas, fornecendo as iscas para as *search-spiders*. Isto resultou, naturalmente, em texto que era muito menos interessante e expressivo, e, na verdade, muito mais penoso e cansativo para ler. Então tinha que ser curto. A qualidade do conteúdo da *Web*, assim, começou a diminuir, e, para manter a atenção do espectador, tinha de ser sempre realizada uma obra artística de gosto popular. O conteúdo da *Web* tornou-se, assim, cada vez mais trivial.

Nesta conjuntura, por meios de *marketing* poderoso, os proprietários dos *search engines* dos Estados Unidos começaram a atrair o maior número de usuários da *Web*. Os *search engines* europeus e outros, rapidamente, caíram de popularidade e acabaram por desaparecer. Mas os principais *search engines* dos Estados Unidos começaram a pensar sobre o mercado. Antes, eles eram meramente serviços auxiliares, prestados internamente por instituições acadêmicas e grandes corporações.

Mas agora eles queriam ganhar lucro. Cobrar de cada pesquisador era essencialmente impraticável. Então eles adotaram um esquema para cobrar dos donos de *websites* comerciais. Um esquema popular foi cobrar dos *websites*, de modo tal que, quanto maior fosse o valor pago em melhor posição ficaria na lista de pesquisa do buscador. Isso resultou em que os *websites* não comerciais praticamente desaparecessem de todas as listas de busca.

Em toda essa confusão, descobri que um pequeno *search engine*, chamado Google, ainda trazia resultados bons e relevantes. Eu penso que, naquela época, talvez Google não tivesse predisposição para cobrar, conforme a posição na lista. Eu não sei. Tudo que eu sei é que os resultados que obtinha eram bons. Finalmente, por qualquer motivo ou por qualquer meio, o Google cresceu e tornou-se o meio *de facto* pelo qual praticamente todos os usuários da Internet, em todo o mundo, procurou *websites* e páginas na *worldwide web*. Assim, o Google tornou-se o único ponto de acesso exclusivo para todas as pessoas no mundo, para obter informação na *worldwide web*.

Isso significa que só o Google pode determinar a forma como toda a *worldwide web* seja indexada a partir do ponto de vista de quase todos os usuários da Internet no mundo. Seu esquema de indexação pode determinar quais *websites* podem ser vistos e quais não podem; quais aparecem nas listas de busca e quais não. Ele pode usar critérios arbitrários, para classificar as páginas da *Web* por relevância, e até excluir vastos trechos de *websites* do seu índice, completamente. Assim, uma única entidade comercial, dentro da jurisdição de um único Estado soberano, tem o controle quase total sobre o fluxo de material intelectual entre todos os habitantes do Planeta Terra.

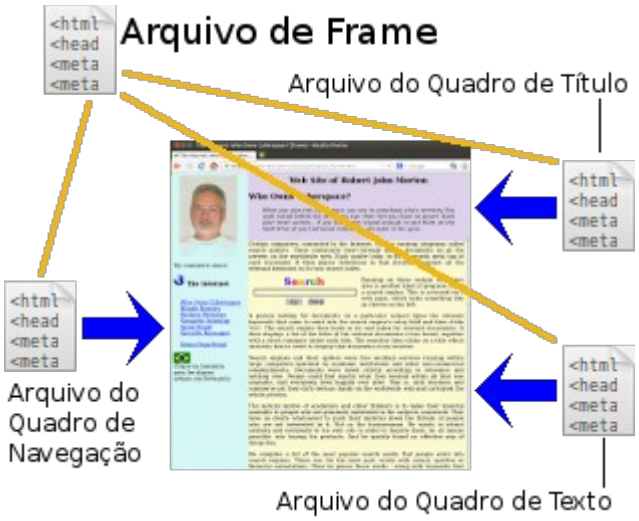
O meu *website* está *on-line* desde abril de 1998. Isto é, antes do Google chegar ao poder. Até por volta de 2004, o meu *website* tinha milhares de visitantes por mês. Recebia centenas de comentários por *e-mail* dos telespectadores. Agora, olhando na lista de acesso, vejo que todo este vasto *website*, de artigos, contendo um total de mais de 1·2 milhões palavras, recebe cerca de meia dúzia de sucessos significativos por mês, tendo sorte. E esses acessos são, exclusivamente, para páginas sobre tópicos técnicos ímpares, que têm importância apenas acessória. Procurando os principais temas dentro deste *website*, utilizando um *search engine*, não revela nada. No entanto, eu tenho cumprido com todas as normas técnicas, que os *search engines* atualmente requerem. Por que deveria estar assim? Estatisticamente, não faz sentido.

A “Aranha” Que é Demasiadamente "Inteligente"

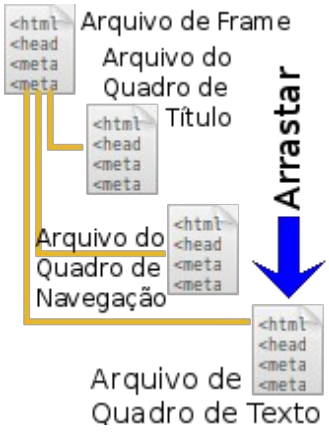
Imagino, que uma das razões para a queda dramática dos acessos a meu *site*, seja que o Google tentou habilitar a sua “aranha” de busca a ser tão mais "inteligente", para "beneficiar" escritores como eu. O que é conhecido como o conjunto de três quadros foi uma forma padrão de apresentação de documentos, do tipo que eu escrevo, desde a antiguidade da Internet.

Cada um dos meus documentos é apresentado, dentro da janela do navegador, em três áreas distintas chamadas quadros. O quadro superior, mostrado na cor rosa, é o Quadro do Título. Ele contém o título do documento, mais um título estendido de 4 linhas ou “declaração de objetivo”. Á esquerda, é o Quadro de Navegação mostrado em azul claro. Este contém hiperlinks para o grupo de documentos de que este documento é uma parte. O quadro restante, em amarelo, é o Quadro do Texto. Ele contém o texto principal.

O conteúdo de cada um dos três quadros está contido em um arquivo separado. Então, são o arquivo do Quadro de Título, o arquivo do Quadro de Texto e o arquivo do Quadro de Navegação. Um quarto arquivo, o Arquivo de Frame, atua como um organizador, para carregar o conteúdo de cada um dos outros três arquivos em sua área apropriada da janela do navegador. Por isto, o documento é mostrado, bastando solicitar que o Arquivo de Frame seja exibido. O próprio Arquivo de Frame faz o resto.



A janela do navegador deve ser idealmente de 840 pixels de largura: 200 para o Quadro de Navegação e 640 para Quadros de Título e Texto. A altura ideal da janela deve ser aproximadamente a mesma ou um pouco mais. Com estas dimensões mínimas, os Quadros de Título e Navegação não rolam. Apenas o Quadro de Texto deve conter uma barra de rolagem vertical. Esse arranjo permite que o leitor role o texto, no Quadro de Texto, para baixo enquanto o título e a declaração de missão ficam, permanentemente, à vista no topo como uma âncora semântica para a mente do leitor, durante a leitura de um longo discurso. O Quadro de Navegação permanece estável também, mantendo o leitor sempre ciente de onde o documento, que está lendo atualmente, se encaixa no grande esquema.



Este arranjo é ideal para apresentar grandes documentos sobre assuntos intelectuais. Não é, no entanto, o que eles chamam de "Google-friendly". Google parece ser completamente confuso com os frames. Inicialmente, como eu entendi, a “aranha” de busca do Google não podia ler JavaScript. Por isto, adotei a seguinte estratégia para induzir Google indexar os meus documentos, a qual explora a incapacidade da “aranha” de busca do Google ver JavaScript.

Eu precisei induzir a “aranha” de busca do Google para arrastar o arquivo do Quadro de Texto do meu documento por palavras-chave. Por isto, apontei todos os links que se referem ao documento em causa, para o arquivo do Quadro de Texto do conjunto de quadros. No

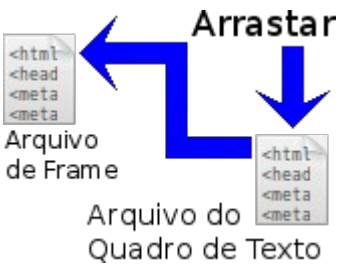
arquivo do Quadro de Navegação e no arquivo de Quadro de Título eu coloquei uma meta tag HTML, no sentido de instruir as aranhas de busca para não indexá-los, mas para acompanhar os links dentro deles, seguindo em diante para outros arquivos. Coloquei uma meta tag diferente no arquivo de Quadro de Texto, instruindo as aranhas para indexar o documento e seguir os links dentro dele para outros documentos.

O que aparece no índice do Google seria, portanto, as referências a cada um dos meus arquivos de Quadro de Texto. Se um pesquisador clicou em um link em uma lista de resultados de pesquisa do Google, o meu arquivo de Quadro de Texto só seria exibido - sem um título, declaração de objetivo ou lista de conteúdos. Isto seria muito deselegante e não seria de muita utilidade. Por isto, eu incluì, na seção de cabeçalho do meu arquivo de Quadro de Texto, a declaração de JavaScript a seguir:

```
if(window==top){top.location.replace("cyberspace_frame.htm");}
```

Isto diz ao navegador que, se ele está solicitando para carregar o meu arquivo Quadro de Texto, como o único documento a exibir na janela do navegador, então, ele deve carregar o arquivo do Frame correspondente deste documento em seu lugar. O arquivo do Frame, em seguida, apresenta os três quadros em suas respectivas áreas da janela do navegador. E está tudo bem.

Ou seja, até que o Google decidiu habilitar a sua “aranha” de buscar a ser “tão inteligente". Parece que o Google deu-lhe habilidade de ler JavaScript. O problema é que, embora a “aranha” do Google possa ser capaz de determinar o que uma declaração JavaScript faz, ela não sabe a razão. E, em sua ignorância, ela assume o pior. Quando encontra a declaração JavaScript acima no início do meu arquivo de Quadro de Texto, ela vê que ele deve ser imediatamente redirecionado para outra página.



Se ela não pudesse ler o JavaScript, cegamente continuaria através do arquivo de Quadro de Texto, para extrair as palavras-chave. Mas ela não faz isto. Ela assume que, por eu redirecioná-la para uma página diferente, é porque eu devo estar fazendo alguma coisa "sorrateira" (terminologia do Google). Por conseguinte, ela recusa a indexar o meu documento. Assim, de milhares de visitantes por mês, as minhas páginas começaram a receber praticamente nenhuma visita.

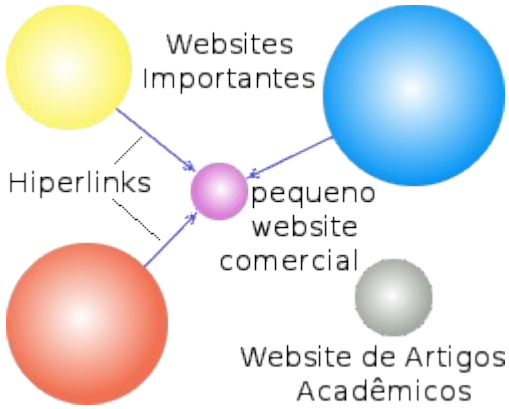
Se a aranha tivesse apenas ignorado JavaScript, tudo ficaria bem. Se tivesse simplesmente obedecido ao JavaScript, executaria o arquivo de quadro para montar o conjunto de quadros, como um documento completo na maneira de um navegador e, em seguida, indexando-o. Mais uma vez, tudo ficaria bem. Mas fazendo apenas parte do trabalho, como fez, Google causou nada mais além de problemas para escritores, como eu.

A minha única saída era criar um *site* paralelo, em que todos os meus 1,2 milhões de palavras dos meus artigos fossem reformatados como documentos entediantes e sem título e sem meios de navegação global do *site*. Então, eu tinha um *site* para os meus leitores e outro para o Google indexar. Que pena. Esperamos que, quando um buscador Google encontre um de meus artigos no formato entediante, ele vá clicar em um link em algum lugar dentro do documento, levando o leitor para a versão do meu *site*, onde está devidamente apresentado. Isto, no entanto, provou não ser uma solução eficaz. Então, eventualmente, tenho que recorrer ao uso de redes não-*Web*, como um meio de fornecer indexação pela porta dos fundos para o meu *site*.

Uma Política de indexação Disfuncional

Apesar do aborrecimento exasperante acima, a razão dominante é que todos os principais *search engines* seguiram o exemplo e mudou seus critérios para *websites* de indexação. Qualquer pequeno *website*, promovendo uma entidade comercial, até uma loja de esquina, é dado um lugar de destaque

nas listas de busca. Para qualquer coisa de natureza intelectual, no entanto, apenas os globalmente conhecidos *websites*, com um alto perfil, aparecem nas listas. Outros parecem ser classificados como sendo de interesse apenas para os seus proprietários e, consequentemente, não são considerados de valor para inclusão numa lista de pesquisa. Claro, outra possibilidade pode ser que os programadores dos algoritmos dos *search engines*, de repente, tornaram-se extremamente ineptos. No entanto, eu não penso que isso seja provável.



Pelo que eu entendo, pelo que eu sou capaz de aprender a partir da *Web*, o principal critério para a prioridade posicional de uma página de *Web* agora é determinado pelo número de *hyperlinks*, que existem para aquela página a partir de outras páginas da *Web*, multiplicado pela "importância" daquelas páginas que contêm estes *hyperlinks*. Sistemicamente, esta política garante, que a alta classificação dos *websites* ,que já estão estabelecidos, é preservada e que nada de novo virá à luz do dia. E isso é, exatamente, o que parece acontecer.

Eu cuidadosamente pesquiso e escrevo um novo documento sobre o que deve ser, pelo menos para algumas pessoas no mundo, um tema interessante. Eu o envio para o meu *website*. Eu o registro dentro do índice do meu *website* e incluo, quando relevante, *hyperlinks* para o meu novo documento dentro das páginas apropriadas, que já estão no meu *website*. O meu novo documento não tem nenhum *hyperlinks*, apontando para ele a partir de *websites* externos. E, portanto, não tem qualquer prioridade posicional dentro do índice de qualquer *search engine*. Ele, portanto, nunca aparecerá em nenhuma lista de busca. Consequentemente, ninguém nunca o verá. Consequentemente, ninguém importante nunca criará um *hyperlink* para o meu novo documento a partir do seu importante *website*. Ele permanecerá, para sempre, excluído. Então, aqueles "pelo menos algumas pessoas no mundo" nunca serão capazes de encontrá-lo, não importa o quão bem sintonizados com um conjunto de palavras-chave, que elas digitaremm no *search engine*. *Quod erat demonstrandum*.

Não obstante o acima, suponho que eu já conheça alguém que esteja muito interessado no tópico sobre o qual eu escrevi. Eu envio a URL do meu novo documento para esta pessoa, para permiti-la acessar o meu documento, diretamente, sem a necessidade de usar um *search engine*. Ele o lerá e gostará. Ele o indicará para outras pessoas. Mas por que ele deveria colocar um *hyperlink* para o meu documento, a partir de outro *website?* Ele pode, simplesmente, marcá-lo no navegador dele. Assim, mesmo que as pessoas fiquem sabendo sobre o meu novo documento por meios, que estão fora da *worldwide web*, é, ainda, não muito provável ser referido a partir de *sites* "importantes".

Assim, se a finalidade é revelar a todos a mina de ouro de informação que está disponível na *worldwide Web*, esta política de indexação é sistemicamente disfuncional. Ela simplesmente preserva a popularidade do que já foi feito popular por outros meios. Mas talvez esta política seja deliberada. Talvez a intenção por trás da mudança no algoritmo de busca, em torno de 2004, foi com o propósito de criar, fortalecer e preservar um estabelecimento da worldwide *Web*, para minimizar, ou mesmo excluir todas os *websites* menores. Antes de 2004, eu poderia pesquisar a *Web* e encontrar uma grande diversidade de coisas interessantes. Agora minhas pesquisas acabam chegando no apropriado *mega-site* estabelecido, o que me mostra apenas conteúdo desinteressante e censurado a que me é destinado ver.

A *worldwide Web* passou, assim, a ser sujeitado a uma forma passiva ou indutiva de censura, efetivada pelo fato de que um *search engine* coloca referências a grandes *websites* estabelecidos no

topo de qualquer lista de resultados de busca, empurrando todos os outros bem abaixo na lista, onde apenas o pesquisador muito diligente vai se preocupar em olhar.

Ordem de Cessar e Desistir

Mas há outra forma de censura, que o governo dos EUA - ou qualquer outra autoridade, agência ou entidade baseada nos Estados Unidos - pode impor aos *websites*. Esta outra forma de censura é um instrumento jurídico chamada ordem de *cessar e desistir*.

Google, que tem sede nos EUA, na confluência de todas as principais rotas dentro da infra-estrutura da Internet em todo o mundo, está, exclusivamente, sujeita a e regulamentada pela lei dos EUA. Se os poderes, quer sejam eles quem forem, não gostarem de algo que foi escrito em uma página da *Web*, eles podem emitir um ordem de *cessar e desistir*. Não ao suposto infrator, isto é, o autor da página, mas ao operador do *search engine*.

A demanda da ordem de *cessar e desistir* não é para excluir a página *Web* em questão ou para excluir o conteúdo "ofensivo" dentro dela, mas para *cessar e desistir* de colocar a página em um índice de pesquisa. Assim, ela nunca aparecerá em qualquer resultado de busca. Desta forma, a localização do servidor do *website*, a nacionalidade do autor da página da *Web* e a jurisdição em particular, dentro da qual ele pode residir atualmente, são todos irrelevantes. O *search engine* está localizado nos EUA e, portanto, está submetido à lei dos EUA, de modo que a execução do ordem de *cessar e desistir* é fácil e simples.

Uma vez eu vi um documento que foi intitulado como um ordem de cessar e desistir dentro de uma lista de pesquisa do meu *site*. Estranhamente, ele parecia ser nada mais do que um modelo. A referência para a ofensiva página da *Web* e o ofensivo conteúdo dentro dela estavam, ambos, em branco. A referida ordem tinha nome e endereço do que, eu presumo, era o escritório de uma advocacia americana. Além disto, a ordem parecia ser nada significante. Pouco tempo depois, ela desapareceu. Eu nunca compreendi esta ocorrência. Presumo que alguém em algum lugar percebeu que aquilo era um equívoco.

O resultado de tudo isto é que o acesso aos conteúdos na *worldwide web* pelo público em geral parece estar, indutivamente, dirigido por um único interesse político, o qual apenas se direciona para o conteúdo que aprova. E o conteúdo destas peças aprovadas parece estar se tornando cada vez mais trivial. Eu não sou nem a favor nem contra os Estados Unidos da América. Eu teria a mesma queixa sendo qualquer outro poder soberano, que tivesse a mesma posição. No entanto, aqui trata-se de uma situação em que um poder soberano, por si só, é capaz de exercer o controle quase total sobre algo que pertence ao mundo inteiro. E é minha firme opinião de que tal situação é fundamentalmente contra os melhores interesses da humanidade.

Velocidade de Acesso Por Grau

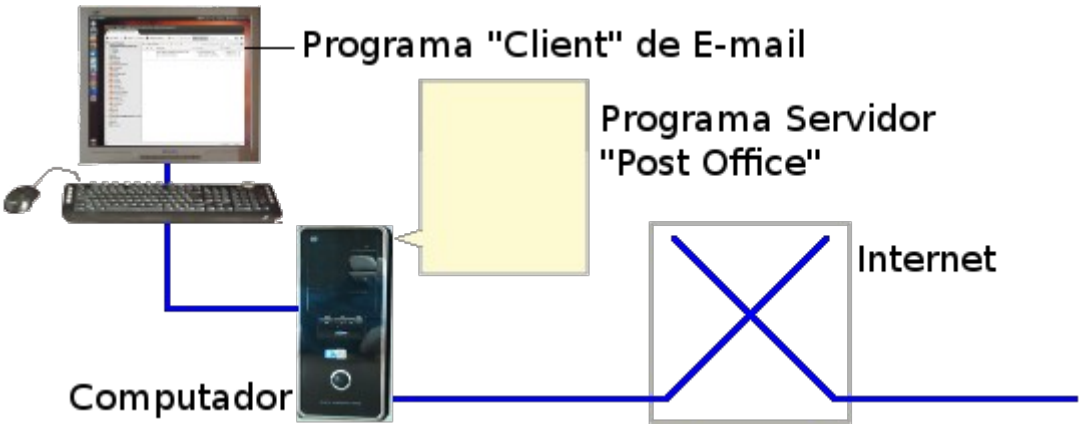
Finalmente, no topo de todas as imposições acima, há mais uma forma indutiva de censura que em breve poderá ser imposta pelos grandes provedores de serviços de Internet. Eles propõem a fornecer velocidades de transferência de dados mais altas para os sites daqueles que são capazes de pagar taxas mais elevadas. Estes irão promover eficazmente os sites comerciais dominantes apoiados por grandes corporações, enterrando sites - não importa o quão alto a qualidade do seu conteúdo - de indivíduos e pequenos grupos que simplesmente não podem pagar essas taxas mais elevadas.

Mas essa sucessão de eventos deve ser de nenhuma surpresa para ninguém. Afinal de contas, ele é simplesmente o capitalismo em ação. Uma vez que a Internet abriu-se ao comércio, sua antiga visão igualitária da liberdade universal para troca de informações nunca foi destinado para durar. Tinha

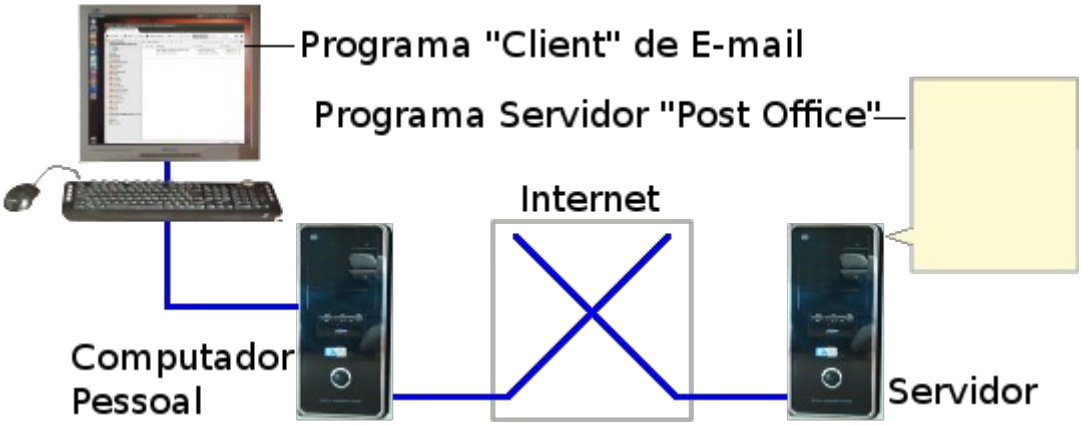
finalmente a entrar no mundo real em que os interesses da maioria são superados pelos interesses dos poucos favorecidos.

E-mail Baseado na *Web*

Antigamente, cada computador, conectado à Internet, tinha um servidor "Post Office" que funcionava 24 horas por dia. Pessoas de todo o mundo poderiam enviar um *e-mail* a qualquer momento para o servidor. O servidor exibia um alerta na tela ao destinatário apropriado, quando um *e-mail* chegava para ele. Ele, então, o acessava e o lia. Assim, o sistema de *e-mail* da Internet foi distribuído e, por consequência, era razoavelmente privado.

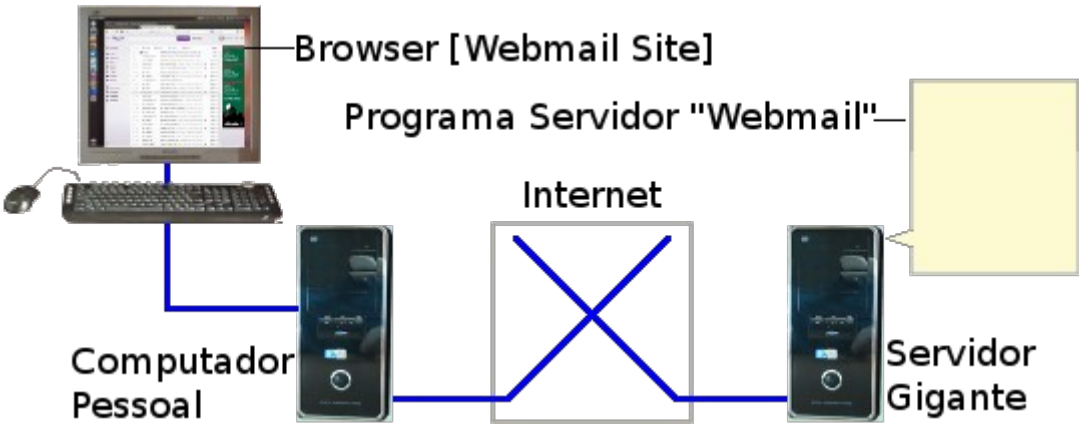


Executar um servidor de *e-mail* requer que computador do destinatário esteja permanentemente *on-line*. Isto foi bom na época em que os clientes da Internet eram grandes máquinas Unix. Logo, porém, pequenos computadores pessoais tornaram-se o mais utilizado pela maioria dos usuários da Internet. Não era nem normal nem desejável que fossem mantidos ligados 24 horas por dia, por tal razão eles não se prestavam como servidores do correio eletrônico. A solução é ter uma distribuição de grandes computadores *on-line*, permanentemente em execução como servidores de *e-mail*. Cada computador pessoal, em seguida, executaria um *client-program* de *e-mail*, que pode acessar o servidor local de *e-mail*, para baixar qualquer novo *e-mail* a qualquer hora. Este é ainda um sistema que é, razoavelmente, bem distribuído.



Sistemas distribuídos são anátema para as autoridades. Isto é, porque eles são difíceis de monitorar e controlar. A solução é atrair pessoas para grandes *websites*, que forneçam um serviço de *e-mail*. Estes *websites* fornecem uma bonita interface de usuário, que é servida através de um navegador *Web*. O usuário de um pequeno computador pessoal faz logon na sua conta em *website* de *e-mail*, para enviar e receber os seus *e-mails*. Os provedores americanos dos *websites* de serviços de *e-mail*

embelezam as suas interfaces de usuário com muitas peças de artes atraentes e anunciam os seus serviços "gratuitos". Diante disto, a grande avalanche de novos usuários de Internet são arrebanhados por eles em todo o mundo, como mariposas numa chama de vela.



O *e-mail* tinha sido originalmente um canal de comunicação sério. Este terminou abruptamente com a chegada dos gigantes serviços-*web* de *e-mail*. Um ethos da trivialidade que se estabeleceu rapidamente. Agora, as pessoas que, não têm nenhum interesse real em *e-mail*, adotam o hábito de encaminhar piadas intermináveis e estúpidas para as pessoas em todo o mundo. O resultado é que as caixas de correio das pessoas tornam-se abarrotadas, a cada dia, com uma quantidade de lixo que poderia encher muitos caminhões. Cada um tem que gastar muito tempo para se livrar de todo esse material indesejado e buscar pelos poucos *e-mails* autênticos escondidos no lixo. Este fenômeno é muito exacerbado pelas avalanches intermináveis do indesejável e, totalmente, abominável propaganda comercial.

Muitas pessoas não conseguem manter o trabalho de filtragem diário necessária para manter as suas caixas de correio livres do lixo. Um vasto número de caixas de *e-mail*, portanto, se torna abandonado, como bolas gigantes de pus purulento, dentro desses servidores de *webmail* megalíticos. Então, quem abandoná-las não têm alternativa senão estabelecer uma nova conta de *e-mail*. E o ciclo repete-se. Que desperdício estúpido de recursos!

Perante neste cenário estressante, a situação é perigosa, em que uma comunicação oficial, tal como um requerimento de pagamento, pode legalmente ser enviado por *e-mail* e, em que sendo remetido, presume-se, legalmente, recebido pelo destinatário. Consequentemente, se o destinatário exclui-lo acidentalmente, juntamente com as centenas de *e-mails* indesejados, entre as quais ele está escondido ou se o *e-mail* foi destinado erroneamente ou se a sua conexão com a Internet ou computador falhou, então o remetente poderia ser penalizado. A meu ver, esta situação é um absurda e completamente injusta.

Ao contrário do programa *client* de *e-mail*, que funciona num computador pessoal, o usuário de um serviço de *webmail* não baixa os seus *e-mails* para o seu próprio computador. Em vez disso, os *e-mails* dele são deixados na sua conta de *e-mail* no servidor gigante do provedor de serviço de *webmail*. Neste servidor, o *e-mail* é armazenado, presumivelmente, de movo privativo. Esta privacidade, porém, permanece somente enquanto a lei americana a permitir, seja em relação à generalidade de pessoas ou à pessoas especificas e em tempos particulares. Assim, não importa a sua nacionalidade ou o seu país de residência, se uma agência do governo dos EUA emite um instrumento legal para o provedor do seu serviço de *webmail*, com sede nos Estados Unidos, para revelar os seus arquivos de *e-mail*, isto será feito.

É bem evidenciado, pela natureza dos *applets* de propaganda, nas bordas da janela do meu navegador, que o provedor de *webmail* vasculha o conteúdo dos meus *e-mails*, em busca de pistas

sobre o que eu seria mais propenso a comprar. Não obstante, é apenas um pequeno passo a partir desta pesquisa vasculhar, também, o conteúdo dos meus *e-mails*, para ver que opiniões ou ligações políticas eu tenho e que sejam dentro ou fora de sintonia com os interesses do governo dos EUA.

No entanto, a facilidade original do *e-mail* da Internet ainda continua. Além disto, penso que o tempo em que cada casa seja equipada com uma rede local doméstica está chegando. Isto será ligado com a Internet, provavelmente, por um pequeno computador de baixo consumo, o qual operará continuamente. Este pequeno computador poderá, então, executar um servidor "Post Office" à moda antiga, de modo que poderá receber e enviar *e-mails* da casa, independentemente, de qualquer serviço de *webmail* megalítico.

Serviços das Redes Sociais

As redes sociais podem ser feitas de modo mais simples e eficazes através de *websites* abertos e *e-mails*. Isto, no entanto, está fora do controle ou influência de corporação e do estado. E isto não é aceitável pelo status quo. Os poderes constituídos - comerciais ou políticos, portanto, definem seu objetivo para induzir a grande maioria dos usuários da Internet a interagir, exclusivamente, através de um pequeno grupo de *websites* das redes sociais dominantes.

Lembro-me das primeiras redes sociais como sendo bastante úteis. Nos início das redes sociais (aproximadamente em 2003), eu poderia usar a MSN para pesquisar e encontrar outras pessoas no mundo que compartilhavam os meus valores, interesses e aspirações. Mas hoje não mais. Os *websites* das redes sociais dominantes hoje, como Facebook, teimosamente, inibem qualquer tentativa que eu faça para ligar-me com pessoas de valores, interesses e aspirações semelhantes. Eu rapidamente descobri que os valores, interesses e aspirações, que eu coloco na minha página do Facebook, não são para ajudar outras pessoas com estes mesmos valores, interesses e aspirações a encontrar-me. Pelo contrário, são, exclusivamente, para ajudar os anunciantes comerciais a fazerem-me de alvo de seus produtos, baseados nos meus interesses registrados. Compreensivelmente, eu saí do Facebook.

As únicas pessoas, com as quais eu jamais fui capaz de articular-me através de uma rede social moderna, foram aquelas que eu já conhecia e os amigos delas. Todas estas pessoas, no entanto, conheceram-se somente através de conexões familiares ou casualmente. De todos os "amigos" que eu acumulei através de redes sociais, nenhum deles compartilhou qualquer um dos meus valores, interesses ou aspirações. E o que eles trocavam um com o outro foi para mim sempre extremamente entediante, trivial e inconsequente.

O resultado é que, para o homem comum, o intercâmbio de informações através da Internet tornou-se impotente, relegando qualquer pensador sério como uma voz que clama no deserto, onde ninguém pode ouvir. Isto deixou a televisão e outros meios de comunicação social, mais uma vez, livres para fazerem lavagem cerebral na mente da maioria das pessoas, levando-as a abandonar o seu próprio bem-estar, para servir ao interesse próprio da elite global. Mais uma vez, apenas aqueles com muito dinheiro, ou seja, o estado e as corporações são capazes de se fazerem ouvidas.

Esta situação não é surpreendente. Para pensadores de mentes semelhantes, por toda a parte do mundo, serem capazes de conectarem-se, através da Internet, para trocarem e desenvolverem ideias, é, inerentemente, perigoso para a elite global. Assim, através das redes sociais, a elite da Internet conseguiu matar dois coelhos com uma só cajadada. A elite da internet reduziu à trivialidade, praticamente, toda a comunicação inter-pessoal entre as pessoas comuns, enquanto, ao mesmo

tempo, transformou estas pessoas numa altamente segmentada audiência capturada para a sua publicidade comercial.

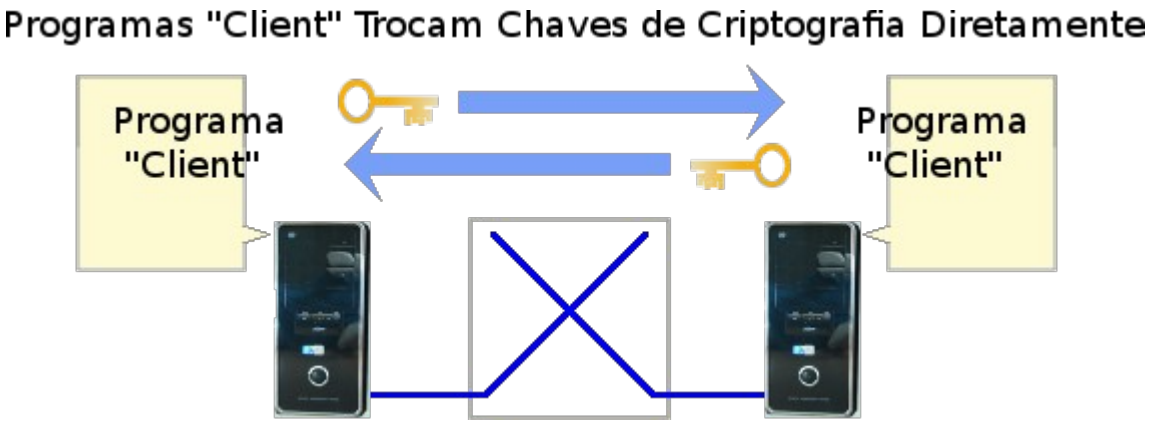
Serviços Centralizados de Bate Papo

Quase desde o início, um método de codificação da voz humana em discretos pacotes do Protocolo da Internet era já comumente disponível, através de um mecanismo chamado de *Internet Relay Chat* (IRC). Há muitos programas *client* gratuitos de fonte livre para IRC, que podem ser baixados e executados em praticamente qualquer computador - pelo menos quem executa uma versão ou derivado do Unix. Estes operam no que é chamado modo peer-to-peer. Uma conversa IRC é conduzida ativamente apenas pelos computadores que pertencem àqueles que participam da conversa. Outros computadores que estejam na rota entre eles são sempre envolvidos passivamente apenas.

Isso permite que duas pessoas, cada uma localizada em qualquer lugar do mundo, participem de uma conversa privada, sem os pacotes de dados, que transportam essa conversa, passando através de qualquer servidor central. Nem as identidades das partes da conversa, nem o conteúdo do que eles dizem podem ser interceptados, monitorados, registrados, interrompidos ou bloqueados por algum interesse de terceiros, tal como uma corporação ou agência governamental. E, para o poder público e corporações tal situação é, simplesmente, inaceitável.

Consequentemente, como acontece com *websites* pessoais e *webmail*, as grandes corporações norte-americanas, logo que surgiram, atuando ativamente, atraíram explosivo número de usuários no mundo da Internet, para estabelecer contas "gratuitas" em seus servidores. O motivo declarado por estas empresas foi, novamente, transformar todas as pessoas do mundo numa grandemente segmentada audiência capturada para as suas respectivas publicidades comerciais.

Com estes serviços baseados em mercado, a criação da conexão entre duas pessoas para um bate-papo, é feita, pelo menos no início, através de um servidor corporativo. Assim, os meta-dados, como as identidades e endereços IP dos participantes na chamada, são conhecidos. Informações a respeito de quem conversou com quem e quando, para os assinantes em todo o mundo, está, portanto, disponível no servidor da empresa. Enquanto isto é muito útil para a comercialização de produtos, talvez seja, ainda, mais útil para a vigilância. E, sendo baseado nos EUA, todos esses servidores corporativos estão sujeitos à lei deste País e, por isto, podem ser forçados a qualquer tempo, por qualquer órgão do governo dos EUA, para divulgarem estas informações.



Os operadores desses serviços de bate-papo da Internet nos asseguram, que a nossa privacidade é sua prioridade e que não precisamos preocupar-nos, porque todas as nossas conversas são

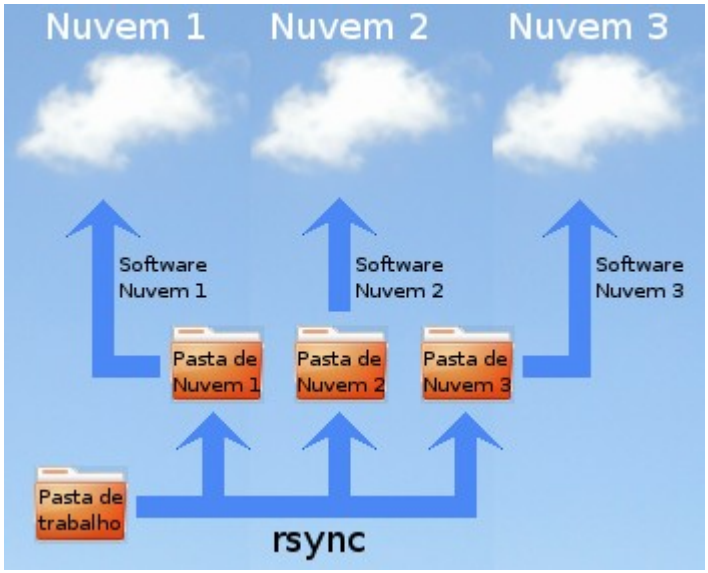
protegidas por criptografia forte. Não obstante, a chave de criptografia de sessão para cada chamada não é criada pelas partes do próprio chamado. Ela é criada pelo software *client* do provedor do serviço, instalados no computador de cada participante. Não há, portanto, nada para prevenir o provedor de serviço para incluir, dentro do seu programa *client*, uma função para enviar a chave ao seu servidor central, se for solicitado por qualquer autoridade.

Além disso, não há nada para impedir o fornecedor do serviço de escolher uma metodologia, que leve o servidor central, e não o software *client*, a criar a chave de criptografia de sessão para cada chamada. Neste caso, qualquer agência, com acesso ao servidor do provedor do serviço, pode escutar qualquer conversa entre quaisquer usuários em todo o mundo. Por este meio, as identidades das participantes de uma conversa e o conteúdo do que dizem, a partir de agora, podem ser interceptados, monitorados, registrados, interrompidos ou bloqueados por algum interesse de terceiro, tal como o prestador do próprio serviço ou por meio de um instrumento jurídico adequado de qualquer agência do governo dos EUA. Se, de fato, eles são capazes de fazer isto, você acredita que eles não fariam?

Sites de "Nuvens" de Armazenamento

Uma "nuvem", neste contexto, é um grande computador mainframe - ou mesmo uma série de tais computadores - que tem uma quantidade muito grande de recursos de armazenamento de dados (como unidades de disco) ligados a ele. Este computador tem acesso à Internet por banda larga de grande capacidade. Qualquer pessoa pode abrir uma conta neste computador através do *site* do provedor do serviço em "nuvem". Isto dá-lhe um montante inicial de espaço de armazenamento gratuito. O usuário pode pedir mais do que isto, mas ele terá, então, que pagar um valor por mês para o espaço extra. Para poder utilizar o serviço de nuvem para fazer backup de seus dados, ele deve baixar e instalar o software *client* do provedor do serviço de nuvem, para executar em seu computador pessoal.

Eu penso, que foi por volta de 2008, que algumas empresas começaram a oferecer quantidades limitadas de armazenamento em nuvem para as pessoas em geral, gratuitamente. Atualmente (início de 2014), sou usuário de três serviços de armazenamento em nuvem, que me autorizam entre 2 a 5 gigabytes de armazenamento gratuito. Eu uso cada um para fazer um backup de segurança fora do local do meu trabalho, que compreende a minha escrita, meu software e minha biblioteca de pesquisa. Isso tudo eleva-se a não mais do que 1,5 GB.



Dentro da minha "home" pasta, eu tenho uma para cada serviço de nuvem. Eu sincronizo minha pasta de trabalho para cada uma das minhas pastas dos serviços de nuvem semanalmente, usando o utilitário de Linux chamado rsync. O software *client* de cada provedor sincroniza a sua pasta com a sua respectiva nuvem. Eu considero ser essencial esta abordagem em duas etapas, para evitar qualquer contratempo na sincronização, em que o serviço de nuvem poderia corromper itens da minha pasta de trabalho. Isso de fato aconteceu antes de eu adotar abordagem em duas etapas.

Computadores-nuvem estão equipados com recursos de armazenamento com alta redundância, a fim de garantir que os dados do usuário sejam sempre recuperáveis. Eles são, portanto, super confiáveis e seguros. Consequentemente, se alguma vez o meu computador pessoal for destruído ou roubado, juntamente com todos os meus backups em casa, eu poderei baixar todo o meu trabalho de um dos meus serviços-nuvem para um novo computador. Essa é o grande e primário valor dos serviços de armazenamento em nuvem.

Qual o motivo que os provedores de serviços de nuvem têm para oferecer armazenamento gratuita às pessoas? A quantidade de armazenamento gratuito, que eles oferecem, é pequeno em comparação com a quantidade atual de armazenamento disponível dentro de um computador pessoal. Até o meu dispositivo móvel está equipado com um cartão de memória de 35GB. A pessoa, em média, tende a usar o espaço que ele tem disponível, principalmente porque ele não se preocupa em apagar documentos desatualizados e fotografias que não saíram tão bem, como desejado. Assim, os arquivos tendem a se acumular no seu dispositivo e encher o espaço de armazenamento disponível. Portanto, como a pessoa usa mais e mais do armazenamento disponível no seu dispositivo pessoal, assim também ela pode querer armazenar uma cópia de segurança. E o armazenamento em nuvem é o lugar ideal para isto. Por ista razão, ela vai rapidamente esgotar a sua subscrição gratuita e precisará comprar mais espaço a partir do seu provedor de serviço de nuvem. Se o usuário do serviço de nuvem é uma empresa, então, certamente o espaço livre será insuficiente desde o início. Assim, a gratuidade do espaço na nuvem é, na verdade, apenas ensaio do aluguel do espaço. Claro que existem algumas pessoas, como eu, que mantém o uso de armazenamento de dados bem controlado, mesmo em seus computadores pessoais. Mas nós somos uma minoria relativamente pequena.

Mas é realmente assim tão simples? Como é possível que todos esses bem-sucedidos prestadores de serviços da nuvem sejam americanos? O resto do mundo, é, então, cheio de ineptos? O que impulsiona essas empresas embrionárias de dois *geeks* para dominar o mundo tão rapidamente? Há muitas pessoas igualmente inteligentes em outros países. Os *geeks*, obviamente, recebem um abundante capital inicial. Eles, obviamente, obtêm assistência administrativa e parecem encontrar, estranhamente, rotas livres de obstáculos que as suas empresas a um crescimento rápido, enquanto que, aqueles de outros países que têm as mesmas habilidades dos *geeks*, no entanto, parecem não ter. Poder-se-ia, portanto, concluir que o que eles fazem é extremamente útil para determinados órgãos, instituições e agências poderosas?

Os meus dados estão seguros, então, quando armazenados numa nuvem? Do ponto de vista da integridade técnica, absolutamente sim. É extremamente improvável que sejam perdidos ou corrompidos. Mas será que é seguro do ponto de vista da privacidade? Se eu armazenar informações pessoais confidenciais em uma nuvem, é possível que qualquer outra pessoa possa acessá-lo? "Não", dizem os provedores do serviço da nuvem. Por quê? Porque todos os meus dados são protegidos por senha. Os meus dados, também, são criptografadas por uma chave que foi gerado a partir da minha senha. E eu sou o único criador da minha própria senha. Um serviço de nuvem diz que até mesmo os seus próprios funcionários não sabem a minha senha. Consequentemente, ninguém pode ter acesso aos meus dados armazenados na nuvem, a menos que eu, deliberadamente, os compartilhe no todo ou em parte.

Não obstante, todas as senhas são armazenadas em algum lugar no computador do provedor dos serviços da nuvem. Todas as senhas podem ser criptografados pelo próprio sistema. Mas o mecanismo de descriptografar deve existir em algum lugar nos computadores do provedor do serviço de nuvem. O mecanismo da descriptografar pode se encontrado e usado por qualquer administrador com privilégios administrativos. De um modo ou de outro, os administradores, operadores, programadores do provedor do serviço da nuvem, entre eles, são capazes de acessar meus dados e descriptografá-los. Agências e instituições governamentais sabem disto.

O prestadores de serviços em nuvem e seus computadores são baseados nos EUA, na confluência do *backbone* global da Internet. Eles estão, portanto, sob a jurisdição da lei dos EUA. Se, portanto, o governo dos EUA ou de uma de suas agências desejarem, por qualquer motivo, ver os meus dados, eles podem emitir um instrumento legal, que obrigue o prestador do serviço de nuvem a fornecer-lhes uma cópia descriptografado dos meus dados armazenados. O governo dos EUA ou qualquer uma de suas agências podem, até mesmo, pedir que o prestador do serviço de nuvem forneça-lhes uma entrada, para o armazenamento em nuvem, por uma porta dos fundos, através da qual eles possam decifrar e inspecionar, à vontade, qualquer todos os dados armazenados na nuvem. No meu caso, penso que seria para eles, extremamente entediante o que encontrarão.

Lembro-me de um comentário num blog, feito por um coordenador de um dos principais prestadores, não-americanos, de serviço de nuvem. Ele afirmou ser altamente recomendável, que nenhum arquivo seja colocado em armazenamento em nuvem, que não seja fortemente criptografado, de antemão, pelo próprio usuário. Esta é uma etapa adicional na minha rotina de backup por semana, que não mencionei acima. Eu sempre crio um arquivo PGP fortemente criptografado de cada um dos meus arquivos de trabalho modificados. Em seguida, copio todos eles dentro de cada uma das pastas no meu computador, as quais são reservadas para arquivos, que serão remetidos, então, para as respectivas nuvens. Desde que as minhas chaves de criptografia PGP não se tornem violadas, isto dá-me grande possibilidade de manter a minha privacidade.

A única outra medida que eu poderia tomar, seria copiar todos os meus arquivos de trabalho modificados em um cartão de memória e criptografá-los, usando um computador off-line que nunca esteja ligado à Internet. Mas isso exigiria muito trabalho.

Para a maioria dos habitantes do Planeta Terra o serviço de armazenamento em nuvem é, provavelmente, a área do ciberespaço em que todos têm a máxima vulnerabilidade à vigilância

clandestina. Isto ocorre porque no seu espaço na nuvem, ao contrário do que se dá com e-mails ou em mídias sociais, todas as suas informações pessoais são armazenadas de uma forma que é essencialmente completa e, também, bem organizada.

O Infiltrado do Seu Computador

Eu vejo o espaço no disco rígido do meu computador, onde os meus dados pessoais são armazenados, como meu território pessoal. Tenho certeza de que a maioria das pessoas, também, veem o mesmo sobre seus computadores pessoais. Antes de os computadores pessoais estarem ligados à Internet, esta visão foi, em grande parte, verdadeira. Era possível infectar um computador pessoal, com o que é conhecido como vírus, via mídia removível, como um disquete. Com um pouco de cuidado e algumas precauções, no entanto, este era evitável. Mas a Internet mudou tudo, no que diz com respeito à segurança dos próprios dados pessoais, dentro do próprio computador pessoal. Hoje em dia, quem sabe quem pode estar bisbilhotando seu disco rígido, “enfiando o nariz” dentro de seus arquivos pessoais? Assim, é melhor evitar armazenamento de assuntos e dados pessoais no seu computador.

Embora fosse possível, os computadores pessoais, antes de 2004, realmente não tinham a velocidade e a capacidade necessária para executar sistemas operacionais do tipo derivado de Unix. A maioria, portanto, não tinha o sistema de privacidade e proteção de uma conta de usuário do Unix com permissão de acesso individual, grupal e geral aos arquivos.

Desde o início, os computadores pessoais operavam, principalmente, com o MS-DOS e, em seguida, com Microsoft Windows. Eu não sei sobre depois de 2008, mas, até então, certamente, estes tiveram pouca ou nenhuma segurança eficaz construído para eles. Segurança, se existiu, foi efetivada por programas de terceiros. Estes programas, freneticamente, “escanearam” o disco rígido e a memória do computador em busca de vírus conhecidos. Outros constituíram "firewalls", que monitoravam os pacotes, que chegavam da Internet para qualquer "atividade suspeita", seja lá qual fosse. Os scanners anti-vírus tiveram que ser atualizados, regularmente, como a guerra entre os produtores dos vírus e anti-vírus, que se alastrou. Isto, naturalmente, resultou em um custo indesejável para os proprietários de computador pessoal.

Os sistemas operacionais já incluíam por longo tempo uma facilidade embutida, para atualizarem-se automaticamente através da Internet. Este sistema automática de atualização sempre foi e é bem protegido contra o uso malicioso por meio de criptografia forte e por troca de certificados digitais. Não obstante, ele dá ao fabricante do sistema operacional uma porta traseira segura, através da qual o fabricante é capaz de acessar todo o seu computador pessoal.

O fabricante do sistema operacional poderia, se ele quisesse, incluir funcionalidade adicional dentro do seu software de atualização automática. Isto poderia facilmente ser um programa para escanear seu disco rígido, a fim de buscar quaisquer dados. O fabricante do sistema operacional é uma empresa americana, que opera dentro da jurisdição dos EUA. Se o governo americano ou qualquer uma de suas agências emitir um instrumento legal, que exija do fabricante do sistema operacional o fornecimento de acesso a qualquer ou a todos os computadores pessoais, o fabricante do sistema operacional não teria escolha senão obedecer.

Com um sistema operacional de fonte fechada em execução no seu computador, você pode não ter nenhuma ideia do que está realmente acontecendo sob a superfície, por trás da interface gráfica do usuário na sua tela. Algum programa poderia estar passando seus dados pessoais, através de uma porta dos fundos para onde só Deus sabe, por motivos da segurança nacional dos EUA.

O próprio sistema operacional não é a única fonte possível de insegurança para a informação privada no disco rígido do seu computador. Os programas de aplicação, também, podem espionar nos seus dados privados. Talvez o maior culpado aqui seja o navegador *Web*. Há, pelo menos, quatro meios, pelos quais um navegador *Web* pode possibilitar obtenção e envio de informações sobre você para um destino desconhecido. Estes são: *cookies*, *plug-ins*, programas JavaScript embutidos em páginas *Web* e controles Active-X.

cookies realmente só reúnem estatísticas sobre seus hábitos de navegação, ou seja, os *sites* que você já visitou. Eles, provavelmente, nem sequer identifica-o como um indivíduo. Eles poderiam passar informação do seu endereço IP. No entanto, o endereço IP do usuário comum muda, pelo menos, a cada vez, que ele inicia seu computador. Um *cookie* é útil na medida em que pode permitir que um determinado *site* "lembre-se" das suas configurações, preferências e senha do *site*. No entanto, o fato de que o *cookie* preservar estes dados, deixa o usuário vulnerável a captura por qualquer agente malicioso escondido dentro do ambiente do navegador.

Um navegador da *Web*, também, pode ter instalados, dentro dele, pequenos programas "ajudantes" chamados de *plug-ins*. Estes permitem o navegador fazer coisas como reproduzir filmes ou fluxos de som, através de objetos embutidos dentro da janela do browser. No entanto, os produtores desses *plug-ins* poderia, facilmente, incluir uma funcionalidade adicional, que não nada a ver com a especialidade do *plug-in*.

Programas de JavaScript e *Applets* Java são programas de computador que são incorporados dentro de uma página da *Web*. Eles são executáveis enquanto a página está sendo exibida. Eles são úteis na medida em que eles podem automatizar formulários, que você precisa preencher em uma página da *Web*. Eu os utilizo para automatizar a ilustração de algumas coisas em outras partes deste *website*.

Programas de JavaScript e *Applets* Java, de acordo com o seu conceito original, são perfeitamente seguros. Tal segurança é explicada, porque eles operam sempre confinados dentro do que é chamado de *sandbox*. Isto significa que um programa de JavaScript ou um Applet Java, fundamentalmente, não pode acessar ou armazenar qualquer coisa no seu computador, fora da própria pasta temporária, porque esta é associada, exclusivamente, ao navegador. Ele pode ler e gravar dados no servidor remoto, a partir do qual a página da *Web* foi exibida. Mas não há, absolutamente, nenhuma maneira de que um programa de JavaScript ou Applet Java possa ver, adicionar ou modificar qualquer coisa em qualquer outro lugar no seu computador, incluindo seus arquivos ou pastas privadas.

Fiquei muito frustrado dois ou três anos atrás, quando eu notei, em um computador do sistema Windows, que o Microsoft Internet Explorer carregava algumas das minhas páginas da *Web*, mostrando um aviso para o usuário, em que dizia que a minha página poderia prejudicar o computador do usuário. Isso, é claro, era uma mentira absoluta. Não há nenhuma funcionalidade dentro do meu código, que pode, eventualmente, prejudicar o computador de qualquer pessoa. Na verdade, o código, em questão, simplesmente exibia na barra de status do navegador, a data em que a página fora modificada pela última vez. Ele nem fez, nem poderia fazer, nada mais. Meu código JavaScript estava lá claramente, para ser visto no código-fonte da página *Web*. Qualquer pessoa com um conhecimento rudimentar de JavaScript podia ver, que ele não poderia causar qualquer dano.

Então, por que o aviso? Só posso especular, que era em razão do seguinte:

1. Microsoft extendeu a capacidade da versão do JavaScript, que havia implementado no seu navegador Internet Explorer, para ser usado de uma tal forma, que poderia vir a prejudicar o funcionamento do computador do usuário e possibilitar acesso dos dados armazenados deste computador;
2. O meio, pelo qual a Microsoft detecta a presença do código do JavaScript em uma página da *Web*, não é suficientemente inteligente para determinar o que o JavaScript realmente faz.
3. O detector do JavaScript da Microsoft adotou uma opção segura, nessas circunstâncias, e, supondo o pior, condenou o meu código do JavaScript como, potencialmente, malicioso. Isto eu entendi como um delito de difamação contra mim, na condição de autor do *website*, na medida em que isto, efetivamente, rotulou-me, colocando-me sob a suspeita dos especialistas de agir, dolosamente, para prejudicar o computador do usuário.

A versão do JavaScript da Microsoft pode ser usada por uma página da *Web*, para baixar e executar controles Active-X. Estes são, efetivamente, programas “nativos”, que operam no seu computador como aplicativos invocados e dirigidos por você. Eles, portanto, não estão confinados na pasta

sandbox do navegador, como estavam nos programas Java e JavaScript, que se conformavam com o conceito original.

Consequentemente, um controle Active-X pode, se fosse projetado para fazê-lo, acessar todo o seu sistema de arquivos, incluindo os seus dados pessoais. Por que introduzir essa vulnerabilidade gritante? Porque facilita algo que muitas pessoas acham útil. Ele facilita às equipes de pessoas usarem os programas-aplicativos, como processadores de textos e planilhas sem demarcações, através de muitos computadores conectados pela Internet, como se fossem um único computador. Mas valeu a pena? Na minha opinião: não, definitivamente.

O resultado do ActiveX é que o perigo pode vir, simplesmente, do seu acesso a um *site* desonesto. O conteúdo do *website*, em si mesmo, pode ser muito bom. Não obstante, uma página *Web* pode conter um programa embutido dentro dele, que é capaz de baixar um programa nativo no seu computador pessoal e ligá-lo no sistema operacional, de modo em que operará sempre que o seu computador estiver ligado. Assim, nem todos os programas baixados fazem isso. Mas poderiam fazer. A capacidade é intrínseca.

Exacerbado Pela Ingenuidade

A vigilância predatória, tanto por potências estrangeiras quanto por ladrões comuns, que acontece através da Internet, é de bom grado assistida pela ingenuidade e credulidade incríveis do público em geral, que, levianamente, rotula todos os dissidentes como paranóicos. Um exemplo particular é como se segue.

Recentemente, os moradores do condomínio de apartamentos onde eu moro decidiram, com grande custo, instalar câmeras de "segurança" em todo o edifício e em volta dele. As imagens da câmera são supostamente visíveis por todos os moradores nos suas computadores domésticos através da Internet. Eu tenho 3 computadores, mais um laptop e um tablet. No entanto, o software de visualização das câmeras, como fornecido pelo vendedor, é incompatível com todos estes meus computadores.

Felizmente, eu descobri uma instalação do Microsoft Windows XP em uma partição antiga e abandonada no disco rígido do meu laptop, que não continha dados pessoais. Eu baixei o software para visualização da câmera e, então, foi-me possível ver as imagens das câmeras. A definição era tão ruim que era impossível identificar qualquer pessoa a partir das imagens. Assim, as câmeras não podem alcançar a sua finalidade de identificar o ladrão.

Qualquer empregado da empresa de segurança, que administra as senhas dos clientes, pode acessar os pontos de vista das câmeras. Esse empregado, fica, portanto, vulnerável a ser subornado para revelar a senha do prédio para um ladrão potencial. Por exemplo, um ladrão poderia pesquisar um empregado particular da empresa de segurança privada. Ele poderia descobrir onde o empregado mora. Ele poderia descobrir onde as crianças do empregado estudam e fotografá-las. Então, ele poderia ameaçar o empregado sobre a "segurança" de sua família, se ele não revelar a senha. O ladrão poderia, então, acessar nossas câmeras através da Internet, assim como nós podemos. O ladrão poderia demorar todo o tempo que ele quisesse para olhar quem vem e quem vai e quando vai. E se para o nosso prédio, por que não para muitos ou mesmo todos os edifícios que assinam ao plano de câmera de segurança?

A senha para olhar as imagens das câmeras foi incluída no documento de instrução sobre como instalar e usar o software de visualização. Este documento estava em um arquivo PDF mantido em um servidor *dropbox*.

O síndico distribuíu o *hyperlink* da *Web* para o referido arquivo PDF em um *e-mail* aberto enviado a cada um dos moradores, revelando os moradores, suas contas de *e-mail* e os respectivos servidores da cada um, tornando, assim, vulneráveis os condôminos. Outros residentes, provavelmente, têm contas de *e-mail* com muitos outros provedores de serviços de *e-mail*. Alguns moradores podem baixar seus e-mails em um software do tipo *client* de *e-mail*. Outros podem acessar seus e-mails diretamente nos servidores da *webmail*.

É sabido que os provedores de serviços de *e-mail* analisam nossos e-mails com o objetivo declarado de marketing direcionado. E quem sabe o que mais para o quem mais? Assim, qualquer funcionário de um provedor de serviços de *e-mail*, com acesso a programas, que analisam e-mails, pode acessar e passar para o link as instruções das câmeras e, portanto, acessar a senha.

Além disso, cada morador, sem dúvida, tem uma lista de contatos dentro de sua conta de *e-mail*, contendo os endereços de e-mails de seus amigos, conhecidos, colegas e vários outros. E todos estes, por sua vez, têm listas de seus respectivos contatos. Usando qualquer técnica de hacking, qualquer um que esteja dentro da pirâmide de contatos do morador, poderia tornar-se caminho de entrada na conta de *e-mail* deste morador.

Uma vez que este *hyperlink* tiver sido adquirido e a senha revelada, qualquer pessoa pode obter o software para olhar as imagens das câmeras, porque isto é um pacote de software geralmente disponível, que requer configuração mínima para atender a cada instalação individual.

Mas isto não é tudo. O software de visualização foi escrito como um controle Active-X., Então, eu fico satisfeito por não ter absolutamente nenhum dado dentro da partição do Windows XP. O controle Active-X é um software de fonte fechada. Por isso, quem sabe quais portas dos fundos estão incorporadas nele pela empresa de segurança ou pelo seu provedor de software? Tecnicamente, é possível para a empresa de segurança, o seu fornecedor de software ou qualquer um de seus empregados da área de informática acessar todas as informações armazenadas no computador, de qualquer dos residentes do condomínio, que tenha instalado o software para visualizar imagens das câmeras.

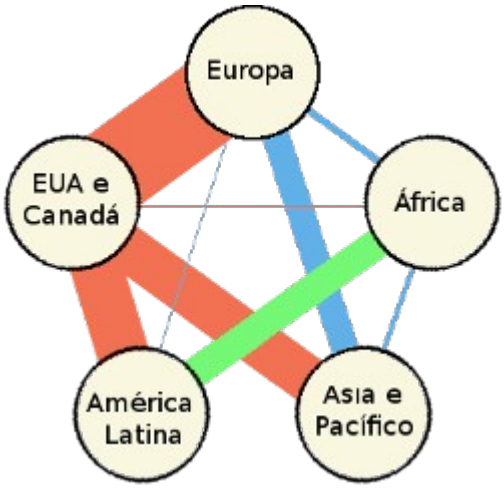
Mas esta não é a única maneira que os dados pessoais dos residentes podem cair nas mãos de criminosos. O síndico envia, a cada mês ao cada morador, um boleto bancário da taxa mensal do condomínio. O boleto bancário é enviado como um arquivo PDF anexado a um *e-mail*. O morador não tem escolha. Ele só pode receber-la desta jeito. O arquivo PDF não é criptografado. Portanto, pode ser lido por qualquer hacker que gere a ganhar acesso à conta de *e-mail* do residente. O boleto bancário não contém apenas o nome do residente e endereço, mas, também, vários outros códigos de identificação e números relativos a essa pessoa. É, portanto, uma fonte principal a partir do qual um criminoso pode construir um perfil completo do residente. Assim, mesmo que, como eu, você seria, naturalmente, tomar todas as precauções sensatas sobre segurança na Internet, pode-se ainda ser forçado, por funcionalismo mesquinho, para deixar-se vulnerável.

Talvez nada de ruim aconteça. Talvez nenhuma pessoa desonesta vai pensar em roubar itens dos moradores ou os seus dados pessoais armazenados nos discos rígidos dos seus computadores pessoais. No entanto, eu penso que é muito estúpido gastar dinheiro dos outros em um sistema que, sem dúvida, contrariamente, reduz a segurança de todos os envolvidos.

Assim, as agências governamentais estrangeiras não são as únicas entidades, que podem meter o nariz dentro dos arquivos armazenados no disco rígido de seu computador pessoal. Assim ,também, podem as empresas privadas, seus funcionários e todo aquele que possa comprometer seus funcionários, incluindo pessoas desonestas. Quanto à Internet, é ingênuo quem pensa que ela não seja um instrumento perigoso. E quem tem tal visão não pode ser confundido como paranóico. No ciberespaço moderno, o computador é como uma casa de vidro em uma terra selvagem, de propriedade e governado por forças saqueadores invisíveis, como a vasta extensão da Ásia submetida pelo medo ao domínio de Gengis Khan.

Uma Política Para Ciberespaço

O altamente assimétrico desequilíbrio na arquitetura atual do *backbone* global da Internet facilita e incentiva o controle totalitário do ciberespaço, pelo governo dos Estados Unidos da América e suas agências. Na minha opinião, isso não é saudável para ninguém - incluindo os próprios americanos. A distribuição total da extensão da banda de dados entre os elos da *backbone* global deveria ser em conformidade com a distribuição da população mundial.



A primeira e mais urgente medida para corrigir este desequilíbrio é estabelecer um Elo Atlântico Sul. Este elo deve ser uma super-rodovia de dados seguros entre o Brasil e a África do Sul, como mostrado em verde, à esquerda. Para garantir a sua robustez, deve-se utilizar das tecnologias de fibra ótica e de micro-ondas, com opções de utilizar tecnologias anteriores, ou seja *fall-back*, como HF, na hipótese da alguma interrupção na rota de alta tecnologia. O Elo Atlântico Sul deve ser construído de tecnologia nativa e de fábrica nacional, ou seja, sem importação, para garantir que nenhum interesse político de fora possa implantar escondidas portas dos fundos dentro da tecnologia do Elo, impossibilitando, assim, que ligações possam ser monitoradas, controladas ou mesmo desligadas à vontade de uma potência estrangeira.

O Elo Atlântico Sul poderia, então, tornar-se a primeira fase do que poderia tornar-se uma *backbone* do BRICS, que liga o Brasil, África do Sul, Índia, Rússia e China. Eu acho que isto se constituiria na maior parte do trabalho para corrigir o desequilíbrio atual. Os nós do *backbone* BRICS tornar-se-íam, então, escolhas naturais, para localizar *search engines* não-americanos e outros recursos de serviços da Internet. Se outros blocos econômicos do mundo, em seguida, promover a homogeneização do *backbone* global, o ciberespaço deve se tornar, progressivamente, o patrimônio comum da humanidade e não a propriedade privada daqueles que governam os Estados Unidos da América.

A existência e o crescimento da Internet demonstram um desejo - que transformou-se em uma necessidade – das pessoas, em todo o mundo, poderem comunicar-se umas com as outras. Isto inclui não apenas a comunicação intelectual entre pares e pares, mas, também, a comunicação coletiva entre o escritor e o público. A Internet respondeu positivamente a este desejo. Ela, no entanto, tem uma perturbadora desvantagem. Ela exige, para o seu funcionamento, uma infraestrutura de alta tecnologia, grande, complicada e cara. E essa infraestrutura é, atualmente, em sua maior parte, propriedade de grandes interesses privados, dos quais muitos deles demonstram um comportamento bastante ruim para o usuário individual. Por exemplo, você já tentou em vão cancelar uma conta com um gigante de telecomunicações?

Seria muito mais confortável e muito menos estressante, se o ser humano, individualmente, pudesse comunicar-se com qualquer um de seus amigos, em qualquer parte do Planeta, por meios naturais - independentemente de qualquer infraestrutura artificial. Uma possível solução seria substituir a Internet por uma espécie de colcha de retalhos global de redes-sem-fio tipo ad hoc. A largura da banda, abrangendo as longas distâncias globais, poderia ser alcançada por enormes quantidades de rotas paralelas.

Um esquema sem fio ad hoc fornece ao indivíduo independência em relação à dominação corporativa. Não obstante, faz cada indivíduo na sociedade ter a obrigação pública de contribuir e participar do referido esquema. Mas isto ainda depende de tecnologias muito complexas, que são de propriedades intelectuais de empresas.

Uma outra opção, a qual, em qualquer caso poderia ser utilizada, como *fall-back*, poderia ser um esquema baseado no serviço de retransmissão na banda de “2 metros” dos radioamadores. Com isto, um rádio amador, inteiramente à sua própria custa, fornece um transceptor operando na banda de “2

metros” dos radioamadores. O transceptor é deixado ligado o tempo todo e retransmite, automaticamente, chamadas de outros radioamadores para a próxima estação. Assim, um radioamador, em uma parte do mundo, pode manter uma conversa com outro, em outra parte do mundo, usando a faixa da banda de “2 metros”, que tem, relativamente, um curto alcance. Este esquema poderia usar relativamente baixa-tecnologia. Equipamento poderia mesmo ser auto-construído pelo usuário entusiasta. Claro que a largura da banda disponível é muito menor do que a Internet ou Wi-Fi fornece. Por outro lado, a grande quantidade de decoração gráfica supérflua, que, inutilmente, flui, diariamente, na Internet, impõe uma sobrecarga enorme na largura de banda requirida, cujo conteúdo da informação significante, de fato, não precisa. A largura da banda de “2 metros” é, certamente, suficiente para realizar um serviço de mensagens curtas ou até mesmo *e-mail*.

Todos os modos de transmissão HF, incluindo uma adaptação adequada de espectro-espalhado, oferece mais uma opção de largura de banda ainda mais estreita, para a comunicação inter-pessoal em todo o mundo. Isto, também, faria uma excelente opção de recuo, no caso em que as opções mais rápidas e mais complexas poderiam falhar. Privacidade para todas essas opções de comunicação, como: Internet, rede-sem-fio ad hoc, VHF (2 metros) e HF, deve ser efetuada por criptografia, de ponta a ponta, estabelecida e mantida pelos usuários individualmente.

Para proteger os interesses de cada usuário dentro de seu computador pessoal, é preciso reverter para os sistemas operacionais seguros da fonte livre. Então, pelo menos, qualquer programador competente no mundo - não importando qual seja o seu pensamento econômico-social - é capaz de ver, com clareza, tudo o que está acontecendo "abaixo da superfície". O que está acontecendo ou poderia acontecer dentro de um computador vai ser, assim, de domínio público e, portanto, estará aberto ao escrutínio da sociedade.

Para garantir ao indivíduo o seu auto-evidente direito de livre acesso a todo o conteúdo da *worldwide Web*, algum tipo de mecanismo global de pesquisa não-censurada é fundamental. Eu penso que isto poderia ser melhor feito de forma distribuída por software de fonte livre, operando numa nova geração de servidores domésticos, que ficariam ligados continuamente.

Atualmente, o *search engine* da *Web* não é mais um meio eficaz de divulgação de discussão intelectual entre as pessoas. Outros meios devem ser desenvolvidos. Talvez o melhor seja converter artigos da *Web* para arquivos PDF, com os nomes dos arquivos, que compõem uma lista de palavras-chave relevantes. Em seguida, lançar estes arquivos em várias redes de compartilhamento de arquivos como Gnutella, eDonkey e Freenet. Interessante observar que, desde que eu lancei os meus arquivos PDF nestas redes, o número de acessos ao meu *website* aumentou muitas vezes. Isto é, provavelmente, resultante da inclusão dentro dos meus arquivos PDF dos hyperlinks, o quais remetem para outras páginas do meu *website*.

Conclusão

Ante tudo o que escrevi acima, por que deveria preocupar-me pelo fato de “o olho que tudo vê” do governo dos EUA e suas agências sejam capazes de lêem os meus e-mails e de espiarem dentro dos meus arquivos privados no disco rígido do meu computador pessoal? Afinal, como muitos são rápidos em responder, "se você não tem nada a esconder, você não tem nada a temer". Não obstante, se devo ou não devo temer, depende mais da natureza dúbia dos motivos e ambições deles do que da minha integridade moral. Portanto, eu poderia, sem o saber, ter muito a temer e, logo, muito a esconder.

Claro, o governo dos EUA não é o único vilão da peça. Muitos outros países têm clandestinas agências, como o Mossad israelense e o tão secreto GCHQ da Grã-Bretanha. Seus motivos e ambições devem ser, pelo menos em certa medida, diferentes daquelas dos EUA. No entanto, nenhum deles, no momento, está na confluência da *backbone* global da Internet. Talvez, se e quando a *backbone* global torna-se mais homogênea, a ameaça à privacidade individual tornar-se-à mais distribuída, equilibrada e, esperançosamente, mais diluída. Eu penso que isto faz-me sentir mais seguro.

Ciberespaço, assim, não tem natureza ou caráter de um Estado soberano, nem mesmo de uma confederação ou de uma aliança política. Tem mais natureza do alto-mar, onde potências marítimas dominantes disputam, para alcançar as respectivas ambições. Mas existe uma diferença. O alto-mar está fora de todos os territórios soberanos. O ciberespaço não. O ciberespaço está em todos os lugares. O resultado é que um Estado Soberano dominante pode determinar que a parte do ciberespaço, que se encontra dentro de seu território soberano, seja governado de acordo com a sua própria lei. Mas isto não o obriga a fazer o mesmo no resto do ciberespaço, que se encontra fora do seu território soberano. Lá ele pode, se assim decidir, agir arbitrariamente, comportando-se como corsário saqueador em alto-mar, livre das limitações de suas próprias leis internas ou, ainda, livre de quaisquer outras leis. Seu comportamento será, portanto, muito provavelmente, determinado pelas estratégias dissimuladas de suas agências secretas.

Qual é o propósito por trás dessas estratégias secretas? O propósito é para colher, por quaisquer meios, justos e injustos, informações, que possam realizar as ambições dos mestres dessas agências. Mas quem são os mestres dessas agências? Eles são uma elite internacional sem rosto, que fecham acordos duvidosos com os senhores da guerra e com os ditadores, que tiram dos pobres de todas as nações as riquezas da Terra, por preço de uma banana. Este processo super-regenerativo de crescente disparidade é inerentemente instável. Ele não pode ser sustentado. Tempo chegará em que a sociedade, tomando consciência de tal situação, destruirá todo este processo, o qual a torna cega, impedindo-a de enxergar a realidade sob a qual vive. Então, a humanidade revolucionará e tomará de volta a sua herança perdida.

This article is also available in English.