A Privacidade na Sociedade da Informação

Carlos Henrique de Fernandes Fernando Mario de O. Filho

8 de dezembro de 2003

"Big Brother is watching you"
George Orwell, escritor inglês, em 1984

"You have zero privacy anyway, get over it."
Scott McNealy, co-fundador e presidente da Sun Microsystems, em 1999

1 Introdução

O surgimento da Internet trouxe à tona questões sobre privacidade que antes não eram relevantes. Questões como até que ponto os dados de uma pessoa podem ser disponibilizados na rede ou até que ponto empresas podem fazer uso de programas capazes de coletar informações sobre seus usuários para alcançar seus próprios objetivos. Onde desenhar a divisória é uma questão ainda em aberto e que está apenas começando a ser discutida. Na Sociedade da Informação, as informações fluem a velocidades e em quantidades há apenas poucos anos inimagináveis, sendo que novas tecnologias estão desencadeando uma verdadeira guerra: de um lado temos meios de nos "intrometer" na vida privada de quase qualquer pessoa que use a Internet, ao passo que novas tecnologias de segunraça estão cada vez mais sendo usadas para garantir a privacidade. Neste trabalho pretendemos exibir um panorama da situação atual e tentar uma possível análise de quais são os caminhos para o futuro.

Nosso objetivo desde o princípio foi tornar este trabalho acessível para um maior número de pessoas, não apenas aquelas familiarizadas com os conceitos e vocabulário de informática. Portanto, procuramos evitar a utilização de termos técnicos, e quando sua utilização foi imprescindível, tentamos explicar de forma simples e clara. Esperamos que o leitor também venha a se interessar pelo assunto, assim como nós nos interessamos.

2 O que é privacidade?

Para investigarmos sobre privacidade temos antes que definir (ou pelo menos tentar definir) o termo "privacidade". Este não é um trabalho simples, já que seu significado é largamente subjetivo: o significado de privacidade para uma pessoa pode diferir por completo do significado de privacidade para outra, mesmo dentro de um mesmo grupo étnico-cultural.

Uma das formas de definir privacidade, sugerida pela comunidade do sítio Privacilla[1] é a seguinte:

[1] O sítio Privacilla é formado através de contribuições de inúmeros autores que discorrem sobre o tema da privacidade com o intuito de dispor informações que podem servir de base para decisões governamentais e de empresas privadas sobre políticas de privacidade. O endereço é `http://www.privacilla.org`.

para ter privacidade, uma pessoa precisa

- ter controle sobre as informações existentes sobre si mesma e
- exercer este controle de forma consistente com seus interesses e valores pessoais.

Existem muitas outras definições de privacidade e muitas outras comunidades na Internet que se dedicam a estudar estes assuntos, tomamos esta definição como um exemplo e também por que ela de certa forma passa a idéia fundamental por trás do assunto.

3 Ameaças a privacidade

Embora seja impossível o anonimato total na rede, devido, principalmente, a especificação do protocolo de comunicação entre os computadores, podemos impedir que a maioria dos nossos dados fiquem disponíveis na Internet.

Mas quais são as ameaças à privacidade presentes na Internet?

As ameças são muitas, porém discutiremos apenas algumas:

- dados transacionais
- cookies
- invasões
- interesses empresariais

3.1 Dados Transacionais

Na Sociedade da Informação, é comum organizações manterem cadastros gigantescos na forma digital sobre seus clientes e parceiros, muitas vezes disponíveis para consultas mediante identificação prévia. Mas esses cadastros não estão isolados, há constantes trocas de informações entre essas bases de dados que crescem assustadoramente dia após dia. Além dessas informações viajando pela rede, há o comércio eletrônico, a simples visita a um sítio, etc. Durante uma conexão, a viagem das mensagens deixam "rastros"pela rede, que permitem uma identificação bem mais detalhada do que se imagina.

A utilização da computação evoluiu muito nas últimas décadas, porém a segurança parece não ter acompanhado essa evolução, principalmente quando trata-se de redes de computadores. Um dos grandes problemas é que os protocolos de rede ainda hoje utilizados foram desenvolvidos décadas atrás, numa época em que segurança contra ataques externos não era muito priorizada, uma vez que poucos tinham condições de adquirir o equipamento necessário para executar tais ataques. Muitos desses protocolos sofreram pouca ou nenhuma modificação, e não garantem a segurança e a inviolabilidade dos dados que são transmitidos, deixando uma grande lacuna para ser explorada por pessoas mal intencionadas.

3.2 Cookies

Os cookies representam violação à privacidade dos usuários da Internet? Esta é uma questão polêmica, discutida em vários sítios da rede, talvez gerada principalmente pela falta de conhecimento dos usuários de como os cookies funcionam e para que servem.

Cookies são simplesmente bits de informação, pequenos arquivos texto geralmente com menos de 1Kb, lançados de um servidor para a máquina do usuário, onde é armazenado no disco rígido.

O arquivo de cookie, a partir do momento que é instalado no disco do usuário, irá guardar alguns dados gerados no servidor web, e pode conter as seguintes informações:

- preferências do usuário para visualização personalizada do sítio, como cores, itens selecionados, menu de navegação, entre outras.
- estatísticas de navegação, guardando quantas vezes o usuário já acessou o sítio, hora dos acessos, etc.
- cesta de compras em sítios de comércio eletrônico, armazenando informações sobre os produtos que estão na cesta do usuário antes da compra ser finalizada.
- controle da exposição de banner, evitando que o usuário veja o mesmo banner mais de uma vez, ou personalizando o banner de acordo com os interesses do usuário.
- preferências temáticas de acordo com a navegação no sítio, para na próxima visita do usuário ao sítio serem exibidos itens relevantes a seus interesses.

As informações citadas acima são as mais comuns, mas dependem muito da criatividade do desenvolvedor do sítio. Os cookies podem ser utilizados para armazenar muitas outras informações.

Os cookies em si estão muito longe de ser uma ameaça à privacidade. O que garante a privacidade do usuário é o fato dos cookies apenas poderem guardar informações que o usuário voluntariamente forneceu ao visitar um sítio, ou informações geradas pelo próprio sítio, além de poderem ser lidos apenas pelo sítio que os criou. Os cookies não conseguem ter acesso a nenhuma informação armazenada no disco rígido do usuário.

3.3 Invasões de computadores

As invasões a microcomputadores da rede, acessando dados particulares e sigilosos, talvez seja a forma mais explícita de invasão de privacidade.

Há falhas de segurança nos sistemas operacionais, que permitem a uma pessoa, com grandes conhecimentos de computação e conhecedora da falha, obter acesso total ou parcial ao computador que esteja rodando o sistema. Um problema gravíssimo, pois normalmente confia-se no sistema operacional e tem-se certeza que os dados armazenados estão seguros, protegidos pela política de segurança do sistema.

Não apenas uma falha no sistema possibilita esta invasão, um sistema mal configurado é um alvo fácil para pessoas mal intencionadas. A Computer at Risk, em 1991, já alertava para este problema. "Na prática, a eficácia de uma proteção depende muito do modo como ela é usada; o melhor cofre do mundo é inútil se ninguém se lembra de fechar a sua porta". Os sistemas operacionais oferecem muitas proteções contra acesso indevido, porém uma configuração incorreta pode comprometer essas proteções e por em risco a segurança de todo sistema.

3.4 Interesses empresariais

Talvez a maior ameaça à privacidade atualmente sejam as empresas privadas, interessadas em "espionar" seus consumidores para serem mais eficientes na venda de seus produtos. Pesquisas de opinião sempre fizeram sucesso entre as empresas para guiar decisões de desenvolvimento de produtos. Neste contexto, a Internet foi vista não só como um potencial novo mercado, como também um novo e poderoso mecanismo para espionar os consumidores.

Sob o pretexto de melhorar a qualidade dos serviços ofertados, muitas empresas distribuem programas pela Internet capazes de fazer estatísticas sobre as páginas visitadas pelos usuários, suas preferências, etc. Este é o caso, por exemplo, do Gator, distribuído pela Internet quando o usuário acessa determinandas páginas.

Embora o Gator só possa ser instalado com a permissão do usuário, muitos dos usuários que não tem tanto conhecimento em computação (ou paciência para ler o contrato do Gator, ficando assim sem conhecer sua finalidade) acabam por instalá-lo. O caso do Gator tem gerado grande polêmica nos Estados Unidos, levantando perguntas a respeito dos limites toleráveis deste tipo de abordagem por parte das empresas privadas.

Também é prática comum entre as empresas trocar livremente informações de seus clientes com parceiros de negócios. Bancos podem trocar informações sobre seus clientes, muitas vezes sem a autorização destes, com outros bancos e empresas. Recentemente, mudanças na lei americana foram propostas para exigir que os bancos só troquem informações dos seus clientes com a permissão expressa destes, mas a pressão por parte dos bancos tem, até o momento, impedido que leis deste tipo fossem aprovadas ou, em certas situações, causado sua alteração de modo a impor condições mais brandas.

Outra questão importante é o funcionamento dos programas proprietários. Como podemos, por exemplo, saber se eles não guardam informações sobre o que fazemos e as enviam pela rede? Políticas de privacidade adotadas por empresas tem se alastrado por estes e outros motivos, mas de qualquer forma no caso de programas proprietários não temos como saber, mesmo que nos assegurem privacidade, que a privacidade é realmente garantida. Se durante a guerra fria temia-se que o Estado espionasse seus cidadãos, hoje com certeza sabemos que as empresas nos espionam. Não por motivos políticos, mas para nos vender mais produtos.

4 Assegurando a privacidade

Embora não haja, na Constituição Brasileira, normas específicas que tratem da privacidade e proteção de dados na Internet, existem dispositivos legais esparsos que protegem a privacidade e sigilo de dados e informações pessoais.

Os princípios gerais do direito de privacidade é assegurada pela Constituição Brasileira de 1988, em seu artigo 5º, inciso X e XII, que prevê o direito a privacidade à medida que garante a inviolabilidade da intimidade, vida privada, honra e imagem de cada cidadão.

> Art. 5º- Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Além das contituições e leis de vários países, são várias as declarações internacionais que defendem a privacidade como direito de todos. A Declaração Universal dos Direitos Humanos, proclamada pela Assembléia Geral das Nações Unidas, e a Declaração de Bogotá , ambas de 1948, já defendiam o direito à privacidade.

Embora esteja sendo muito discutida nos últimos anos, a preocupação em assegurar a privacidade não é recente. O maior agravante, e que tem dificultado muito a garantia de segurança, é a crescente entrada de novas tecnologias nas vidas das pessoas, o que vem agilizando cada vez mais a comunicação e a troca de informações entre pessoas e organizações.

É cada vez maior o número de pessoas que faz compras através da internet, que possui informações pessoais em sistemas médicos, bancários, de advogados, entre outros, além dos próprios dados que as pessoas divulgam em páginas pessoais. São dados disponíveis na rede global. Embora muitos desses

sistemas garantem a segurança e a inviolabilidade dos dados que mantêm, existe o perigo constante de ataques "hackers"[2], que pode por em risco a privacidade do indivíduo.

4.1 Criptografia

Durante milhares de anos, reis, rainhas e generais dependeram de comunicação eficientes de modo a governar seus países e comandar seus exércitos. Para a comunicação à distância, era necessário enviar mensagens através de intermediários, e era extremamente importante manter a confidencialidade. Todos estavam cientes das conseqüências de suas mensagens caírem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. O destinatário desejava ter privacidade em sua comunicação.

Foi esta busca pela privacidade que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só pessoas autorizadas possam ter acesso ao seu conteúdo.

Criptografia é a ciência que estuda técnicas de transformação de dados, para que eles se tornem ininteligíveis para pessoas desautorizadas, mas que seja possível a reversão dessa transformação, permitindo o acesso aos dados de indivíduos autorizados.

4.1.1 Tipos de Criptografia

Existem 2 tipos principais de criptografia:

- **Chave[3] Secreta**

  Neste tipo de criptografia, utiliza-se uma chave secreta para criptografar os dad os. A chave é o "segredo", quem conhecê-la conseguirá descifrar a mensagem e obter os dados originais. A criptografia é de chave secreta porque a chave deve ser mantida em segredo tanto pelo remetente quanto pelo destinatário para para proteger a integridade dos dados. Como a mesma chave é usada para cifrar e decifrar a mensagem, este tipo também é conhecido como algoritmo de chave simétrica.

- **Chave Pública**

  O maior problema da criptografia de chave secreta é a distribuição da chave, que deve ser combinada previamente. Porém normalmente as partes envolvidas na comunicação pretendem usar a criptografia porque o canal de comunicação que irão utilizar não é seguro, e não disponibilizam de nenhum canal seguro. Qual seria a solução?

  A brilhante idéia surgiu em 1975: utilização de chaves assimétricas[4]. O que torna esse tipo de criptografia especial é que a chave de cifragem e decifragem não são idênticas. A dificuldade de distribuir a chave estava resolvida.

  Cada pessoa possui um par de chaves, a chave pública e a chave privada.

[2] "Hacker" (não possui tradução para o português) é o usuário que possui aptidão técnica, prazer em resolver problemas e superar limites. Este termo começou a ser utilizados pelos estudantes do MIT (Massachusetts Institute of Technology) para designar aqueles usuários que "fuçavam" nos computadores da Universidade além dos limites de uso.

[3] Chave corresponde a sequência de caracteres (um nome, uma palavra, uma frase, etc) que permite, mediante o algoritmo de encriptação, cifrar ou decifrar uma mensagem.

[4] Vale a pena enfatizar, que embora Whitfield Diffie tenha concebido a idéia geral de uma criptografia assimétrica, ele não conhecia uma que pudesse demostrar sua idéia na prática.

4.1.2 Criptografia no mundo

À medida que entramos no século XXI, os defensores das liberdades civis começam a defender o uso generalizado da criptografia de modo a proteger a privacidade dos indivíduos. Porém, ao mesmo tempo, as forças da lei defendem um uso mais restrito da criptografia. O que é mais importante para os indivíduos, a privacidade ou uma força policial mais eficiente?

Durante décadas os serviços policiais e de espionagem têm usado a escuta telefônica e interceptação de mensagens para reunir provas contra grupos do crime organizado e terroristas, mas o desenvolvimento recente e acelerado de códigos difíceis de serem quebrados pode enfraquecer essas ações. Embora atualmente a criptografia tenha um impacto maior nas atividades civis, ela ainda é vital para proteger informações militares.

Em 1952, os americanos criaram uma agência de Segurança Nacional (National Security Agency - NSA), com o objetivo de centralizar e liderar todos os esforços do governo para proteger os sistemas de informação norte-americanos. Para garantir a interceptação e o monitoramento das comunicações, a agência tem controle sobre as tecnologias de encriptação desenvovidas pelas empresas americanas, e é severa quanto a exportação dessas tecnologias.

Além de impor restrições a exportação dessas tecnologias, o governo norte-americano também pressiona os demais países desenvolvidos a adotarem medidas semelhantes, aderindo a tratados internacionais extremamente restritivos.

As restrições tendem a ser adotadas por outros países. No início de dezembro de 2002, representantes de 33 países reuniram-se em mais uma rodada do Acordo de Wassenaar para discutir os mecanismos de controle de exportação de armas e de tecnologias associadas. O objetivo é limitar a exportação de tecnologias sensíveis, que incluem não só armamentos militares como também tecnologias de uso civil que possam também ser utilizadas para guerra ou terrorismo, com destaque para a criptografia. Cada país se compromete a alterar sua própria legislação para se adaptar aos termos do acordo.

O Brasil não está entre esses 33 países, e parece estar priorizando a privacidade dos cidadãos, ao contrário de outros países que estão defendendo a segurança da nação. No decreto nº3.505, de 13 de junho de 2000, o governo assumiu publicamente a importância da segurança da informação instituindo a política de segurança da informação nos órgãos e entidades da administração pública federal. O decreto também assegura a garantia a privacidade do indivíduo nos termos previstos na Constituição Brasileira.

Outros países já mudaram explicitamente de posição quanto ao controle da utilização da criptografia. Um desses países é a França, que por muito tempo restringiu sua utilização, porém reverteu sua política em janeiro de 1999 e anunciou que seus cidadãos poderiam utilizar criptografia sem restrições. A Bélgica, em dezembro de 1997, também alterou sua lei que restringia uso da criptografia.

Ainda não há um conceso internacional, porém a larga disponibilidade da criptografia na Internet dificultará a adoção de políticas de restrição por alguns países e a livre utilização por outros. Será impossível forçar o cumprimento de leis restritivas sem a imposição de uma vigilância em massa através de um orgão de censura.

5 Políticas de Privacidade

Atualmente é extremamente comum informarmos nossos dados pessoais em grandes sítios, seja para receber notícias periodicamente através do nosso e-mail, para ganhar acesso ao conteúdo exclusivo do sítio, ou mesmo para simples cadastramento. O usuário conhece as políticas de privacidade dos sítios? Essas políticas são claras? Quantos sabem como proteger suas informações pessoais?

O Centro de Privacidade Pública da Universidade da Pensilvânia (EUA) pesquisou os extensos documentos legais publicados em vários sítios. Estes documentos informam as políticas de segurança e privacidade adotadas pelos sítios. O resultado, divulgado em julho de 2003, é surpreendente.

A pesquisa focou-se nos norte-americanos adultos que acessam a internet de suas casas (as pessoas que acessam apenas do trabalho foram excluídas). A pesquisa foi realizada através de entrevistas por telefone (com duração aproximada de 20 minutos), sorteado-se os números aleatoriamente, onde foram consultados 1.200 adultos maiores de 18 anos.

Concluiu-se que os norte-americanos compreendem mal a finalidade das políticas de privacidade, embora a maioria dos entrevistados possuam grau elevado de escolaridade. Mesmo aqueles que têm consciência que sua navegação está sendo rastreada, e que informações pessoais estão sendo fornecidas, não se preocupam como essas informações podem vir a ser utilizadas. Na verdade, quando informados que os sítios costumam guardar informações sobre seus clientes, dizem que isto é um fato inaceitável.

A pesquisa também mostrou alguns dados curiosos:

- 57% dos entrevistados acreditam incorretamente que quando um sítio possui uma política de privacidade, este sítio não irá compartilhar as informações dos usuários com outros sítios e organizações.

- Embora 47% dos norte-americanos afirmam que as políticas de privacidade são de fácil compreensão, 67% desses 47% também acreditam (erroneamente) que sítios com políticas de privacidade não irão compartilhar os dados dos usuários.

- 85% dos adultos norte-americanos que acessam a internet de casa não concordam que seus dados sejam colhidos pelos sítios, nem mesmo os que oferecem serviços pagos. 54% dos pesquisados responderam que preferiam pagar para continuar com acesso anônimo ou até obter a informação em outro lugar, fora da Web.

- Dentre esses 85% que disseram não concordar com as políticas, mais da metade confidenciou já ter informado em sítios pagos seus nomes e endereços eletrônicos reais.

- Embora toda essa preocupação com a privacidade online, 64% afirmaram nunca ter procurado informações sobre como proteger suas informações na rede. Apenas 9% dos entrevistados disseram saber como evitar que os sítios coletem suas informações pessoais.

- 86% acreditam que leis que obriguem as políticas de privacidade dos sítios a possuirem um formato padrão ajudarão os usuários a se protegerem melhor contra essa coleta de informações pessoais.

Joseph Turow, autor do relatório "Americans and Online Privacy: The System is Broken"onde foi publicado o resultado da pesquisa, aponta, que apesar das políticas terem como principal objetivo a proteção legal dos sítios, elas acabam confudindo ainda mais o usuário, que normalmente não têm idéia do que acontece por trás da tela de seu microcomputador. No final do relatório, ele sugere que os sítios deveriam ser obrigados a divulgar suas políticas em linguagem clara, detalhando o que eles sabem sobre os visitantes, o que fizeram com aquelas informações pessoais e o que planejam descobrir com a coleta de tais dados.

6 Tendências

Como será o futuro? Iremos caminhar para uma sociedade onde os indivíduos não possuirão nenhuma privacidade? O avanço acelerado da tecnologia da informação está causando impacto na esfera social, econômica e cultural, e vêm gerando discuções sem precedentes. Tenta-se analisar a atual situação e como será o futuro da humanidade.

Norton Godoy[5] acredita que a invasão de privacidade "é resultado de um movimento mundial, aparentemente sem volta, que restringe cada vez mais nosso direito à privacidade toda vez que as chamadas tecnologias da informação são aperfeiçoadas."A reportagem "The surveillance society"publicada na revista britânica The Economist, compartilha a mesma opnião de Godoy. Segundo a reportagem "as novas tecnologias da informação oferecem imensos benefícios - alta produtividade, melhor prevenção ao crime, melhora no atendimento médico, diversão interativa, comodidades. Mas vêm com um preço: menos e menos privacidade."

No artigo "The Digital Imprimatur", extremamente pessimista, John Walker[6] descreve como a internet pode se tornar cada vez menos livre. Ele acredita que a internet não é mais uma rede livre ponto a ponto, mas é composta de 2 redes, uma é composta dos produtores de conteúdo, que possuem os servidores, e a outra rede é composta pelos usuários, que estão sentados atrás de firewalls[7] e apenas consomem o conteúdo. Critica os certificados digitais, que embora já implementados, só estão acessíveis para as organizações devido seu preço elevado. Apresenta também as consequências potencialmente negativas da Plataforma Computacional Confiável (Trusted Computing) como Palladium[8], na qual o usuário deverá confiar que não está sendo dominado pelo pessoal que desenvolve o sistema operacional.

Phil Zimmermann[9] também discursa sobre a ameaça de perda da privacidade. Observa a facilidade de interceptação das mensagens eletrônicas, que pode ser feita automaticamente, e indetectavelmente em grande escala, e que isto já está sendo feito pela NSA. Neste mesmo artigo, "Why do you need PGP?", Zimmermann questiona por que pessoas comuns e organizações políticas populares não têm tido acesso à tecnologia criptográfica de chave-pública de nível militar, e seu objetivo quando escreveu o PGP era exatamente dar o poder às pessoas para ter o controle de sua privacidade. Alerta que "se a privacidade se tornar ilegal, somente criminosos terão privacidade".

Richard Stallman[10] descreve a política de segurança das universidades na segunda metade do século XXI. O que tempos atrás seria apenas uma história de ficção científica, pode se tornar realidade. Stallman mostra o dilema de Dan Halbert após Lissa Lenz pedir para utilizar seu computador. Cada livro tinha embutido um monitor de copyright que informava quando e onde ele era lido, e por quem, para a Central de Licenciamento, que utilizava estas informações para descobrir piratas de leitura e também vender perfis de preferências dos leitores. Lissa não poderia ler os livros que estavam no computador de Dan, pois certamente a SPA (Software Protection Authority) descobriria e Dan seria severamente punido por não ter feito os sacrifícios necessários para evitar o crime. O autor fala sobre a batalha pelo direito de ler e sobre a vigilância eletrônica. A política de segurança está acima da privacidade do indivíduo.

Já há esforços para que a proteção ao indivíduo e à liberdade de informação sejam garantidos. Nesse sentido, já surgiram organizações de proteção, como o Electronic Privacy Center e o Center for Democracy and Technology, que batalham pela conservação do anonimato no ciberespaço. Também já

[5]Norton Godoy é editor-assistente de ciência e tecnologia da Revista IstoÉ online.

[6]John Walker é um dos criadores do software CAD da empresa Autodesk.

[7]Um firewall é uma barreira inteligente normalmente entre uma rede local e a Internet, através da qual só passa tráfego autorizado. Esta barreira impossibilita, na maioria das vezes, o acesso a rede interna.

[8]O projeto Palladium, uma parceria entre Microsoft, Intel e AMD, anunciado em agosto de 2002, refere-se a um novo conjunto de características do sistema operacional Windows que, quando combinadas a um novo hardware e novas aplicações, dariam aos usuários maior segurança nos dados, maior privacidade e maior integridade do sistema

[9]Phil Zimmermann é um engenheiro de software com mais de 20 anos de experiência, especialista em criptografia, segurança, comunicação de dados e sistemas embutidos de tempo real. Foi o criador do PGP (Pretty Good Privacy), um software de criptografia de mensagens eletrônicas mais conhecido do mundo.

[10]Richard Stallman é fundador do projeto GNU, iniciado em 1984 para desenvover o sistema operacional livre GNU. Foi o principal desenvolvedor do gcc (GNU Compiler Collection), um compilador portável que atualmente roda em 30 plataformas diferentes, e de outros programas GNU, como o gbd (GNU symbolic debugger) e o editor Emacs. Estima-se que esses programas estão sendo usados por 20 milhões de pessoas em todo o mundo.

há propostas de estabelecimentos de padrões a serem adotados pelos sítios, como o P3P (Plataform for Privacy Prefences Project), que está sendo desenvolvido pelo W3C (World Wide Web Consortium), a entidade que regulamenta a maioria dos padrões na Internet. O Projeto de Plataforma para Preferências Privadas (P3P) fornece uma maneira simples e automática dos usuários manterem o controle sobre o uso de suas informações pessoais nos sítios visitados.

Esta guerra para preservação da privacidade contra a vigilância permanente do indivíduo parece estar muito longe do fim. Muitos argumentos estão sendo utilizados para defender um ou outro ponto de vista, e muitas leis e regulamentações deverão ser criadas e alteradas para adequar-se a nova realidade.

É visível a invasão cada vez maior da privacidade, porém nem todos estão dispostos a cruzar os braços e aceitar que isso aconteça. De um lado temos as autoridades defendendo a invasão na privacidade dos indivíduos para a garantir a própria segurança da nação e empresas querendo perfis de seus clientes para vender mais produtos e do outro temos os indivíduos que não desejam que todos seus passos sejam monitorados, e estejam sujeitos a cairem em mãos alheias.

Os seres humanos aprendem através de sua interação social o que temer e em que confiar. A ameaça à privacidade como estamos vendo agora é muito nova e as próprias pessoas que podem ser suas potenciais vítimas não a reconhecem como tal. Estamos vivendo uma revolução rápida, somos tão fortemente impulsionados por ela (e ao mesmo tempo a impulsionamos com tal força) que muitas vezes não temos tempo de decidir se uma mudança é boa ou ruim. Talvez no futuro as pessoas serão menos acostumadas com a privacidade que conhecemos hoje, não notando a diferença em relação ao passado. Falar do futuro é, entretanto, complicado. De onde estamos, o futuro parece nebuloso na melhor das hipóteses. Só podemos esperar que, no final, não percamos toda nossa privacidade, pois parte dela já foi irreversivelmente perdida.

7 Referências

1. *Privacilla.org*. [online] Disponível na Internet via WWW. URL: `http://www.privacilla.org`. Sítio consultado em 18 de novembro de 2003.

2. *cookiecentral.com*. [online] Disponível na Internet via WWW. URL: `http://www.cookiecentral.com/`. Sítio consultado em 30 de novembro de 2003.

3. CHAVES, Dagoberto L. M. de Miranda. *Cookies não violam privacidade de usuários da Internet*. [online] Disponível na Internet via WWW. URL: `http://conjur.uol.com.br/textos/22655/`. Arquivo capturado em 30 de novembro de 2003.

4. TUROW, Joseph. *Americans and Online Privacy: The System is Broken*. [online] Disponível na Internet via WWW. URL: `http://www.appcpenn.org/04_info_society/2003_online_privacy_version_09.pdf`. Arquivo capturado em 18 de novembro de 2003.

5. GODOY, Norton. *Cuidado! Sua privacidade está sendo invadida*. [online] Disponível na Internet via WWW. URL: `http://www.terra.com.br/istoe/especial/156221.htm`. Arquivo consultado em 15 de novembro de 2003.

6. YOSHIDA, Elias Y. *Segurança, Criptografia, Privacidade e Anonimato*. [online] Disponível na Internet via WWW. URL: `http://www.ime.usp.br/~is/ddt/mac339/projetos/2001/demais/elias/`. Arquivo consultado em 14 de novembro de 2003.

7. SINGH, Simon. *O Livro dos Códigos*. Rio de Janeiro: Record, 2001.

8. TERADA, Routo. *Segurança de dados*. São Paulo: Edgard Bluncher, 2000.

9. *Constituição da República Federativa do Brasil de 1988*. [online] Disponível na Internet via WWW. URL: `http://www.planalto.gov.br`. Sítio consultado em 29 de novembro de 2003.

10. *Decreto nº 3.505*. [online] Disponível na Internet via WWW. URL: `http://www.mre.gov.br/portugues/ministerio/legislacao/diversos/dec3505.html`. Arquivo consultado em 29 de novembro de 2003.

11. *Wassenaar Arrangement*. [online] Disponível na Internet via WWW. URL: `http://www.wassenaar.org/docs/docindex.html`. Sítio consultado em 29 de novembro de 2003.

12. *The National Security Agency* . [online] Disponível na Internet via WWW. URL: `http://www.nsa.gov/`. Sítio consultado em 29 de novembro de 2003.

13. *Cryptography and Liberty 2000*. [online] Disponível na Internet via WWW. URL: `http://www2.epic.org/reports/crypto2000/overview.html`. Arquivo consultado em 29 de novembro de 2003.

14. UGARETTI, Ricardo. *O uso de software livre em criptografia: razões históricas*. [online] Disponível na Internet via WWW. URL: `http://www.comciencia.br/reportagens/guerra/guerra22.htm`. Arquivo consultado em 29 de novembro de 2003.

15. UGARETTI, Ricardo. *Relato de Experiências sobre Desenvolvimento de Software Livre*. [online] Disponível na Internet via WWW. URL: `http://www.mct.gov.br/Temas/SL/pdf/SL_Casnav.pdf`. Arquivo capturado em 29 de novembro de 2003.

16. *Wikipedia*. [online] Disponível na Internet via WWW. URL: `http://en.wikipedia.org/`. Sítio consultado em 29 de novembro de 2003.

17. WALKER, John. *The Digital Imprimatur*. [online] Disponível na Internet via WWW. URL: `http://www.fourmilab.ch/documents/digital-imprimatur/`. Arquivo consultado em 29 de novembro de 2003.

18. *Philip Zimmermann's Home Page*. [online] Disponível na Internet via WWW. URL: `http://www.philzimmermann.com/index.shtml`. Sítio consultado em 29 de novembro de 2003.

19. ZIMMERMANN, Phil. *Why do you need PGP?*. [online] Disponível na Internet via WWW. URL: `http://www.pgpi.org/doc/whypgp/en/`. Arquivo capturado em 29 de novembro de 2003.

20. *Richard Stallman's Personal Home Page*. [online] Disponível na Internet via WWW. URL: `http://www.stallman.org/`. Sítio consultado em 29 de novembro de 2003.

21. STALLMAN, Richard. *The Right to Read*. [online] Disponível na Internet via WWW. URL: `TheRighttoRead`. Arquivo capturado em 29 de novembro de 2003.

22. *Platform for Privacy Preferences (P3P) Project*. [online] Disponível na Internet via WWW. URL: `http://www.w3.org/P3P/`. Sítio consultado em 30 de novembro de 2003.