MANIFESTO **CYPHERPUNK**
(1993)†

Eric Hughes

Privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto privado é algo que não desejamos que o mundo inteiro saiba enquanto um assunto secreto é algo que ninguém quer que qualquer pessoa saiba. Privacidade é o poder de se revelar seletivamente ao mundo.

Se duas partes têm algum tipo de negociação, então cada uma tem uma memória de sua interação. Cada parte pode falar a partir de sua própria memória sobre isto. Como alguém poderia evitar isso? Pode-se aprovar leis contra ela, mas a liberdade de expressão ainda é fundamental para uma sociedade aberta, até mais que a privacidade; procuramos não restringir qualquer discurso. Se muitas partes falam juntas no mesmo fórum, cada uma pode falar com todos os outros e agregar conhecimento sobre indivíduos e outras partes. O poder das comunicações eletrônicas permitiu tal conversação em grupo, e ela não vai embora apenas porque poderíamos querer.

Uma vez que desejamos privacidade, devemos garantir que cada parte de uma transação tenha conhecimento apenas do que é diretamente necessário para essa transação. Uma vez que qualquer informação pode ser falada, devemos garantir que revelamos o mínimo possível. Na maioria dos casos, a identidade pessoal não é saliente. Quando eu compro uma revista em uma loja e entrego dinheiro para o funcionário, não há necessidade

† *Tradução:* Coletivo Cypherpunks, disponível em: https://cypherpunks.com.br/biblioteca/o-manifesto-cypherpunk/ com revisão de Victor Wolffenbüttel. O original, em inglês, está em https://nakamotoinstitute.org/cypherpunk-manifesto/ .

de saber quem eu sou. Quando peço ao meu provedor de e-mail para enviar e receber mensagens, ele não precisa saber a quem estou falando ou o que estou dizendo ou o que os outros estão dizendo para mim. Meu provedor só precisa saber como obter a mensagem lá e quanto eu devo-lhes em taxas. Quando minha identidade é revelada pelo mecanismo subjacente da transação, não tenho privacidade. Eu não posso aqui me revelar seletivamente; *sempre* devo me revelar.

Portanto, a privacidade em uma sociedade aberta requer sistemas de transações anônimas. Até agora, o dinheiro foi o principal sistema. Um sistema de transação anônima não é um sistema de transação secreta. Um sistema anônimo capacita os indivíduos a revelar sua identidade quando desejado e somente quando desejado. Esta é a essência da privacidade.

Privacidade em uma sociedade aberta também requer criptografia. Se eu disser algo, quero que seja ouvido apenas por aqueles para quem eu pretendo dizê-lo. Se o conteúdo do meu discurso está disponível para o mundo, eu não tenho privacidade. Criptografar é indicar o desejo de privacidade, e criptografar com criptografia fraca é não indicar muito desejo de privacidade. Além disso, revelar a identidade com certeza quando o padrão é anonimato requer a assinatura criptográfica.

Não podemos esperar que governos, corporações ou outras organizações grandes e sem rosto nos concedam privacidade por benevolência. É para benefício próprio que falam de nós, e devemos esperar que eles vão falar. Tentar impedir a sua fala é lutar contra as realidades da informação. A informação não apenas quer liberdade, ela deseja ser livre. As informações se expandem para preencher o espaço de armazenamento disponível. A informação é a prima mais jovem e mais forte do rumor; a informação é rápida com os pés, tem mais olhos, sabe mais, e compreende menos do que o rumor.

Devemos defender nossa própria privacidade se esperamos ter qualquer uma. Temos de nos unir e criar sistemas que permitam transações anônimas. As pessoas têm defendido sua própria privacidade por séculos com sussurros, escuridão, envelopes, portas fechadas, apertos de mão secretos e mensageiros. As tecnologias do passado não permitiam a privacidade forte, mas as tecnologias eletrônicas sim.

Nós, os Cypherpunks, estamos dedicados a construir sistemas anônimos. Estamos defendendo nossa privacidade com criptografia, sistemas anônimos de encaminhamento de e-mails, assinaturas digitais e dinheiro eletrônico.

Cypherpunks escrevem códigos. Sabemos que alguém tem de escrever software para defender a privacidade, e uma vez que não podemos ter privacidade a menos que todos nós tenhamos, vamos escrevê-lo. Nós publicamos nosso código para que nossos companheiros Cypherpunks possam praticar e brincar com ele. Nosso código é gratuito para todos, em todo o mundo. Não nos importamos muito se você não aprovar o software que escrevemos. Sabemos que o software não pode ser destruído e que um sistema amplamente disperso não pode ser desligado.

Os Cypherpunks não se importam com regulamentos sobre a criptografia, pois ela é um ato privado. O ato de cifrar, na verdade, remove informações do domínio público. Mesmo as leis contra a criptografia alcançam apenas a fronteira de uma nação e o braço de sua violência. A criptografia se espalhará inelutavelmente por todo o globo junto com os sistemas de transações anônimas que ela possibilita.

Para que a privacidade seja generalizada, ela deve fazer parte de um contrato social. As pessoas devem se unir e juntas implementar esses sistemas para o bem comum. A privacidade se estende tanto quanto a cooperação entre seus companheiros na sociedade. Nós os Cypherpunks procuramos perguntas e preocupações

e esperamos que possamos engajar nossos companheiros de sociedade para que não nos desapontemos. Não seremos, no entanto, afastados do nosso curso porque alguns podem discordar dos nossos objetivos.

Os Cypherpunks estão ativamente empenhados em tornar as redes mais seguras para a privacidade. Vamos avançar juntos.

Avante.

Eric Hughes
<hughes@soda.berkeley.edu>
9 de Março de 1993