ARMAS E FERRAMENTAS

O FUTURO E O PERIGO DA ERA DIGITAL

BRAD SMITH
PRESIDENTE DA **MICROSOFT**

E **CAROL ANN BROWNE**
DIRETORA SÊNIOR DE COMUNICAÇÕES E RELAÇÕES EXTERIORES DA **MICROSOFT**

ALTA BOOKS
EDITORA
Rio de Janeiro, 2020

SUMÁRIO

Prefácio de Bill Gates *xv*

Introdução: A NUVEM:O Arquivo do Mundo *xix*

Capítulo 1: VIGILÂNCIA: Um Estopim Prestes a Estourar *1*

Capítulo 2: TECNOLOGIA E SEGURANÇA PÚBLICA:
"Prefiro Ser um Perdedor do que um Mentiroso" *21*

Capítulo 3: PRIVACIDADE: Um Direito Humano Fundamental *39*

Capítulo 4: SEGURANÇA CIBERNÉTICA: O Sinal de Alerta para o Mundo *61*

Capítulo 5: PROTEGENDO A DEMOCRACIA:
"Uma República, se Conseguirmos Mantê-la" *77*

Capítulo 6: MÍDIAS SOCIAIS: A Liberdade que Nos Afasta *89*

Capítulo 7: DIPLOMACIA DIGITAL: A Geopolítica da Tecnologia *109*

Capítulo 8: PRIVACIDADE DO CONSUMIDOR: "Levantar a Guarda" *131*

Capítulo 9: BANDA LARGA RURAL: A Eletricidade do Século XXI *151*

Capítulo 10: A FALTA DE TALENTOS: O Lado Humano da Tecnologia *169*

Capítulo 11: IA E ÉTICA: Não Pergunte o que os Computadores Podem Fazer, Pergunte o que Eles Devem Fazer *191*

Capítulo 12: IA E RECONHECIMENTO FACIAL: Nossos Rostos Merecem a Mesma Proteção que Nossos Celulares? *211*

Capítulo 13: IA E MÃO DE OBRA: O Dia em que o Cavalo Perdeu Seu Posto de Trabalho *231*

Capítulo 14: ESTADOS UNIDOS E CHINA: Um Mundo Tecnológico e Polarizado *249*

Capítulo 15: DEMOCRATIZANDO O FUTURO: A Necessidade de Uma Revolução Open Data *269*

Capítulo 16: CONCLUSÃO: Lidando com uma Tecnologia Maior do que Nós *287*

Notas 305

Índice 335

Capítulo 1

VIGILÂNCIA: Um Estopim Prestes a Estourar

Quando o sol matinal de verão se despojou das nuvens no dia 6 de junho de 2013, em Redmond, Washington, Dominic Carr abriu um pouco mais as folhas da persiana em seu escritório do quinto andar, no campus da Microsoft. Como o verão no noroeste do Pacífico demora um mês para chegar, os raios de sol que atravessavam a sua janela eram uma provocação bem-vinda aos dias mais quentes — e ao ritmo um pouco mais lento — que estavam por vir.

Ele pegou o celular e desceu de elevador para comprar um sanduíche no café da empresa ao lado. Enquanto caminhava pelo trajeto movimentado entre os edifícios, seu celular, que estava no bolso de trás, vibrou. Dominic encabeçava a equipe de relações públicas e comunicação, e respondia a mim, lidando com alguns dos problemas mais espinhosos da empresa em relação à mídia. Ele nunca ficava sem o celular — e dificilmente ficava longe de sua mesa.

Uma notificação de e-mail — "Microsoft/PRISM" — pisca em sua tela. Na época, "PRISM" era o que chamávamos de encontro anual dos lí-

deres de venda da empresa. Apenas mais uma comunicação de rotina sobre os negócios cotidianos da Microsoft.

Mas este não era um e-mail habitual. Era o estopim de um problema que logo explodiria ao redor do mundo.

"Estamos escrevendo para notificá-lo de que o *Guardian* está se preparando para publicar na noite de hoje um artigo sobre o PRISM — um programa secreto e voluntário de cooperação entre diversas empresas tecnológicas de grande porte dos EUA e a NSA", começava o e-mail, referindo-se à Agência de Segurança Nacional nos Estados Unidos.

O e-mail vinha de outro Dominic — Dominic Rushe — um repórter do jornal britânico *The Guardian*. A princípio, a mensagem chegou à caixa de entrada de um gerente de relações públicas da Microsoft em Boston, que o encaminhou com o status de alta prioridade — uma tag de e-mail com um ponto de exclamação que basicamente dizia: "Vocês precisam ver isso agora."

O texto incluía uma lista complexa com nove pontos para análise e ditava um prazo impossível. Rushe explicava que "como jornalistas responsáveis, gostaríamos de lhes dar a oportunidade de responder a quaisquer inverdades nos pontos enumerados acima. Já abordamos a Casa Branca em relação a esta história. Devido ao caráter delicado do programa, esta é a primeira oportunidade que tivemos de entrar em contato com vocês para que possam apresentar suas observações". Ele queria uma resposta até 18h no horário de verão da Costa Leste, ou até 15h no fuso horário de Seattle.

O *Guardian* teve acesso a documentos de informações confidenciais que detalhavam como nove empresas de tecnologia dos EUA — Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL e Apple — haviam pretensamente se inscrito em um programa voluntário, chamado PRISM, facultando à NSA acesso direto a e-mail, bate-papo, vídeo, fotos, detalhes de redes sociais e outras informações.

Os planos de Dominic para o almoço — e para os próximos dias — foram deixados de lado. Ele deu meia-volta e apressadamente subiu as esca-

das, dois degraus de cada vez, de volta ao quinto andar. Ele suspeitava que esse problema tivesse relação com um artigo alarmante publicado naquela manhã pelo *Guardian*. O jornal publicara um despacho em segredo de justiça que exigia que a gigante norte-americana de telecomunicações Verizon entregasse às autoridades governamentais, "diária e continuamente", seus registros de ligações feitas tanto internamente como entre os Estados Unidos e outros países.[1] Os registros foram analisados pela NSA, sediada em Fort Meade, Maryland, que há muito tempo coletava sinais de inteligência (SIGINT) e dados em todo o mundo. Segundo o artigo, essa coleta em massa também tinha como alvo milhões de norte-americanos, a despeito de terem feito alguma coisa errada ou não.

Se alguém da Microsoft sabia do PRISM, esse alguém era John Frank, o advogado que cuidava das equipes jurídicas, inclusive do nosso trabalho de segurança nacional. Dominic foi imediatamente ao escritório de John.

Sempre comedido e metódico, John assimilou aos poucos a mensagem do *Guardian* no celular de Dominic. Ele tirou os óculos, afastou-se de sua mesa e olhou fixamente para o dia pincelado pelo sol. De repente, ele parecia esgotado. "Isso não faz o menor sentido. Nada disso parece certo."

John não apenas sabia como e o que a empresa analisava e apresentava às autoridades, mas também ajudou a elaborar esse processo. A Microsoft divulgava os dados dos clientes somente em resposta a processos legais válidos — e no que dizia respeito às contas ou pessoas específicas.

Quando John e Dominic chegaram à porta do meu escritório, eles tinham pouco mais para compartilhar do que a mensagem do repórter. "Se eles estão fazendo isso, é sem o nosso conhecimento", afirmou John.

Sim, éramos obrigados a analisar e a responder à solicitação de dados de usuários de acordo com a lei. Tínhamos um procedimento estabelecido com o objetivo de analisar meticulosamente e responder a todas as solicitações do cumprimento da lei. No entanto, a Microsoft é uma empresa gigante. Isso teria sido obra de um funcionário desonesto?

Logo descartamos essa hipótese. Conhecíamos nossos sistemas internos e procedimentos para receber, analisar e responder às exigências do governo. A notificação do *Guardian* simplesmente não fazia sentido.

Ninguém na Microsoft tinha ouvido falar do PRISM. O *Guardian* estava relutante em divulgar os documentos vazados nos quais vinha trabalhando. Entramos em contato com pessoas que conhecíamos na Casa Branca, e elas também não falavam ou compartilhavam nada que fosse "confidencial". No decorrer da tarde, cogitei com John e Dominic: "Talvez façamos parte de um clube secreto, mas tão secreto, que nem sabemos que somos membros."

Teríamos que aguardar até que a história fosse publicada para começar a responder ao repórter.

Às 15h do horário de verão da Costa Leste, o *The Guardian* publicou sua notícia bombástica: "O Programa PRISM da NSA Tem Acesso aos Dados dos Usuários da Apple, Google e Outros".[2] Finalmente soubemos que PRISM, o programa de vigilância eletrônica de segurança nacional da NSA, era um acrônimo para Planning Tool for Resource Integration, Synchronization and Management [Ferramenta de Planejamento para Integração, Sincronização e Gerenciamento de Recursos].[3] Quem tinha inventado esse nome prolixo? Parecia o nome de um produto ruim do setor tecnológico. Segundo a mídia, era um programa de vigilância eletrônica para rastrear dispositivos móveis, chamadas, e-mails, conversas online, fotos e vídeos.[4]

Em poucas horas, o artigo do *Guardian* e reportagens semelhantes do *Washington Post* repercutiram em todo o mundo. Nossas equipes de vendas e advogados foram bombardeados com ligações de clientes.

Todos eles perguntavam a mesma coisa: aquilo era verdade?

De início, não estava claro onde a mídia estava conseguindo aquelas informações. As pessoas discutiam se elas eram mesmo verídicas. Mas, três dias depois, o jornal divulgou uma notícia quase tão bombástica quanto a reportagem. O *Guardian* revelou sua fonte,[5] a pedido dele mesmo.

A tal fonte era um funcionário de 29 anos da consultoria de segurança Booz Allen Hamilton. Seu nome? Edward Snowden. Ele era contratado no Threat Operations Center da NSA, no Havaí, como administrador de sistemas. Após fazer o download de mais de 1 milhão de documentos altamente sigilosos,[6] em 20 de maio de 2013 embarcou em um voo para Hong Kong, onde se reuniu com jornalistas do *Guardian* e do *Washington Post* e começou a compartilhar os segredos da NSA com o mundo.[7]

No segundo semestre daquele ano, os documentos de Snowden se transformavam em uma série de reportagens. O primeiro documento vazado foi uma apresentação em PowerPoint sigilosa de 41 slides, usada para treinar o pessoal dos serviços de informações. E isso era apenas o começo. Os repórteres explorariam o esconderijo de arquivos secretos de Snowden no ano seguinte, estimulando a inquietação por meio de uma onda constante de manchetes. Um tsunami de desconfiança pública se formava face às reivindicações dos Estados Unidos e do Reino Unido para acessar os registros telefônicos e dados de usuários, inclusive informações referentes a líderes estrangeiros e a milhões de norte-americanos inocentes.[8]

As notícias deixaram a sociedade com os nervos à flor da pele, e com razão. As declarações contrariavam abertamente as proteções de privacidade que as sociedades democráticas tinham como garantidas por mais de dois séculos. Esses direitos, em que nos baseávamos para proteger informações na atualidade em nosso data center de Quincy, se originaram no século XVIII durante uma controvérsia turbulenta nas ruas de Londres. O homem que fomentou a tempestade política era um membro do próprio Parlamento. Seu nome? John Wilkes.

John Wilkes foi, sem sombras de dúvidas, o político mais intempestivo — e radical — de seu tempo. Na década de 1760, ele não apenas confrontou o primeiro-ministro, mas também o rei com palavras tão grosseiras que fariam com que alguns políticos de hoje (quase) se envergonhassem. Em abril de 1763, Wilkes escreveu uma crítica anônima em um jornal da oposição. O artigo enfureceu o procurador-geral britânico Charles Yorke, que suspeitava que o autor fosse Wilkes, e logo o governo emitiu um

mandado de busca e apreensão tão abrangente que as autoridades policiais tinham jurisdição para procurar basicamente em qualquer lugar e a qualquer momento.

Agindo deliberadamente, com base em informações inconsistentes, eles entraram na casa de um editor suspeito no meio da noite, "arrancaram-lhe da cama que dormia com a esposa, apreenderam todos os seus documentos pessoais e prenderam quatorze jornaleiros e empregados".[9] As autoridades britânicas apressadamente revistaram mais quatro casas, prendendo um total de 49 pessoas, quase todas inocentes. Derrubavam as portas, vasculhavam baús e arrombavam centenas de cadeados.[10] Em algum momento, reuniram provas suficientes para capturar o homem que queriam; John Wilkes foi preso.

Mas Wilkes não era do tipo que aceitava as coisas de braços cruzados. No período de um mês, ele entrou com uma dúzia de processos judiciais e foi a tribunal para contestar as autoridades mais poderosas do país. Embora isso não tenha sido de se espantar, o que aconteceu a seguir escandalizou o *establishment* britânico e, sobretudo, o próprio governo: os tribunais decidiram a favor de Wilkes. Indo na contramão de séculos de poder exercido pelo Rei e seus homens, os tribunais exigiam que as autoridades tivessem maior causa provável a fim de empreender uma busca e apreensão e, mesmo assim, que a fizessem de modo mais limitado. A imprensa britânica aclamou as decisões, citando a famosa frase de que "a casa de todo inglês é o seu castelo e não pode estar suscetível à averiguação, tampouco à indiscrição de seus documentos, pela crueldade perniciosa dos mensageiros do Rei".[11]

Em diversos aspectos, os processos judiciais de John Wilkes assinalaram o nascimento dos direitos de privacidade modernos. As pessoas livres invejavam esses direitos, incluindo os colonos britânicos que viviam na América do Norte. Apenas dois anos antes, eles haviam empreendido — e perdido — um litígio igualmente intenso na Nova Inglaterra, em que, antes mesmo de advogar em juízo, John Adams, quase chegando aos 30 anos, estava sentado nos fundos de um tribunal de Bos-

ton para assistir a um dos maiores confrontos do continente no início da década de 1760. James Otis Jr., um dos advogados mais impetuosos de Massachusetts, protestava contra as tropas britânicas que exerciam poderes semelhantes contra os quais Wilkes se opôs. Como os vendedores locais contrabandeavam produtos importados sem pagar impostos, os quais consideravam injustos, os britânicos reagiam aplicando os denominados mandados gerais que os autorizavam a ir de casa em casa procurando violações de clientes sem provas específicas.[12]

Otis alegava que isso era uma violação fundamental dos direitos civis, chamando-a de "a pior instância do poder discricionário".[13] Ainda que Otis tenha perdido o processo, suas palavras marcaram o primeiro passo dos colonos rumo à insurreição. No fim de sua vida, Adams ainda se recordaria da alegação de Otis e escreveria que "ela havia soprado nesta nação o fôlego da vida".[14] Até a data da sua morte, ele afirmava que o processo daquele dia, naquela sala do tribunal referente àquela questão, definiu o caminho dos Estados Unidos rumo à independência.[15]

Levariam treze anos, após a Declaração de Independência, para o princípio que Otis defendia tão fervorosamente se transformar em realidade. Até então, a questão fora transferida para Nova York, onde o primeiro Congresso dos EUA se reuniu em Wall Street, em 1789. James Madison compareceu diante da Câmara dos Deputados e apresentou sua proposta de Declaração de Direitos.[16] Eles contemplavam o que se tornaria a Quarta Emenda à Constituição dos Estados Unidos, assegurando que os norte-americanos tivessem a garantia de proteção de suas "pessoas, casas, documentos e pertences" contra "buscas e apreensões arbitrárias" por parte do governo, incluindo o uso de mandados gerais.[17] Desse modo, as autoridades eram obrigadas a comparecer a um juiz independente e evidenciar "causa provável", a fim de obter um mandado de busca para uma residência ou escritório. Na prática, isso significa que o governo deve demonstrar a um juiz que existem fatos que levariam "uma pessoa de inteligência mediana" a acreditar que um delito está sendo cometido.[18]

Mas essa proteção se estende a informações que saem de sua casa? A Quarta Emenda foi colocada à prova, depois que Benjamin Franklin inventou os correios. Você lacra um envelope e o entrega a uma agência do próprio governo. No século XIX, a Suprema Corte não teve problemas para descobrir que as pessoas ainda tinham direito à privacidade em suas correspondências lacradas.[19] Como resultado, a Quarta Emenda era válida, e o governo não podia abrir um envelope e procurar alguma coisa sem um mandado de busca e apreensão com base em causa provável, ainda que ele estivesse nas mãos do serviço postal do governo.

Ao longo dos séculos, os tribunais verificavam se as pessoas tinham uma "expectativa razoável de privacidade" e consideravam a relevância disso quando se armazenavam informações com outra pessoa. Em termos simples, se a informação estivesse em um contêiner de armazenamento trancado e a chave estivesse longe do alcance de outrem, os juízes concluíam que essa expectativa existia e aplicava-se à Quarta Emenda. No entanto, se você armazenasse seus documentos em uma caixa de arquivos empilhados, próxima às caixas de outras pessoas que iam e vinham, a polícia não precisava de um mandado de busca e apreensão. Os tribunais concluíam que você abria mão de sua expectativa razoável de privacidade de acordo com a Quarta Emenda.[20]

Os data centers fortificados de hoje, com níveis exagerados de segurança física e digital, parecem se encaixar devidamente na descrição de contêiner de armazenamento trancado.

No segundo semestre de 2013, éramos sempre pressionados por um repórter atrás do outro, no encalço da história de Snowden, baseada em um documento confidencial vazado recentemente. A mesma rotina. Quando vi Dominic encolhido no escritório de John, soube que outra história estava prestes a ser publicada. Boa parte das vezes, nem sequer sabíamos ao que estávamos respondendo. "Nas primeiras semanas, eu conversava a mesmíssima coisa com um repórter diferente quase todos os dias", lembrou Dominic. "Eles diziam: 'Veja bem, Dominic, alguém está mentindo. Ou é a Microsoft ou é o Edward Snowden.'"

As denúncias do *Guardian* sobre o PRISM retratavam somente uma parcela de uma longa história acerca das tentativas da NSA de obter dados do setor privado. Conforme detalhavam minuciosamente os documentos revelados agora,[21] nos dias posteriores à tragédia do 11 de Setembro de 2001, a agência buscou parcerias voluntárias junto ao setor privado para coletar dados de usuários, além de procedimentos legais de intimação e mandados judiciais.

A Microsoft, como outras empresas líderes em tecnologia, hesitou em fornecer esses dados voluntariamente ao governo. À medida que conversávamos internamente a respeito dessas questões, estudávamos a situação geopolítica mais abrangente. A sombra pesada dos ataques de 11 de Setembro pairava sobre o país. As forças da coalizão deram início à Operação Liberdade Duradoura (OEF-A) no Afeganistão; o Congresso estava apoiando a invasão do Iraque; e a sociedade civil norte-americana, assustada, exigia iniciativas mais rigorosas contra o terrorismo. Foi um período inimaginável. Como muitos disseram, exigia uma resposta sem precedentes.

Mas existia um problema essencial em pedir às empresas que entregassem, de forma voluntária, informações como as descritas nas denúncias reveladas ao público. Os dados solicitados pela NSA não pertenciam às empresas tecnológicas. Eles eram de propriedade dos clientes, e a grande maioria deles incluía informações pessoais.

Assim como o programa PRISM, as tentativas da NSA de obter voluntariamente informações do cliente do setor privado após o 11 de Setembro suscitaram uma pergunta fundamental: como podemos cumprir nossa responsabilidade com os clientes enquanto atendemos a solicitações para proteger o país?

Para mim, a resposta é clara. O Estado de Direito deve se encarregar dessa questão. Os Estados Unidos são uma nação governada por leis. Se o governo norte-americano quer os registros de nossos clientes, precisa acatar a lei do país e recorrer ao tribunal para obtê-los. E, caso as autoridades

do poder executivo achem que a lei não tem alcance o suficiente, elas podem recorrer ao Congresso e exigir mais jurisdição. É desse modo que uma república democrática deve funcionar.

Ao mesmo tempo em que em 2002 não poderíamos ter previsto Edward Snowden e sua famosa fuga, poderíamos ter examinado a história com o objetivo de prever, de um modo geral, o que o futuro poderia nos reservar. Em períodos de crise nacional, a troca das liberdades individuais pela segurança nacional não é nenhuma novidade.

A primeira crise do país aconteceu pouco mais de uma década depois da assinatura da Constituição. Era 1798, quando uma "quase guerra" estourou entre os Estados Unidos e a França, no mar do Caribe. Os franceses, querendo pressionar os Estados Unidos a quitar os empréstimos que pediram a seu rei deposto, confiscaram mais de trezentos navios mercantes norte-americanos e exigiram resgate.[22] Alguns norte-americanos enfurecidos clamavam por uma guerra aberta. Outros, como o presidente John Adams, achavam que a nova nação não era páreo para os franceses. Com medo de que a discussão política arruinasse mortalmente o governo inexperiente, Adams tentou reprimir a discórdia assinando um conjunto de quatro leis, que ficaram conhecidas como as Leis do Estrangeiro e de Sedição. Essas leis permitiam ao governo encarcerar e deportar estrangeiros "perigosos", e criticar o governo se tornou crime.[23]

Mais de sessenta anos depois, durante a Guerra Civil Americana, os Estados Unidos renunciaram novamente a um princípio fundamental de nossa democracia, quando o presidente Abraham Lincoln suspendeu o mandado de *habeas corpus* diversas vezes a fim de subjugar as rebeliões confederadas. Para assegurar o recrutamento do exército, Lincoln estendeu a suspensão e negou o direito de julgamento em todo o país. Ao todo, cerca de 15 mil norte-americanos foram mantidos na prisão durante a guerra sem comparecer perante um juiz.[24]

Em 1942, logo após o bombardeio de Pearl Harbor, o presidente Franklin D. Roosevelt, influenciado pelas Forças Armadas e pela opinião

pública, assinou um decreto que forçava 120 mil norte-americanos de ascendência japonesa a viverem em campos distantes, enjaulados por arame farpado e guardas armados. Dois terços desses prisioneiros nasceram nos Estados Unidos. Quando o decreto foi anulado, três anos mais tarde, a maioria perdera suas casas, fazendas, negócios e comunidades.[25]

Embora o país admitisse essas injustiças em momentos de crise nacional, os norte-americanos depois contestavam o preço que pagavam pela segurança pública. Na minha cabeça, a questão era: "Como seremos julgados daqui a dez anos, quando esse momento passar? Seremos capazes de afirmar que honramos nosso compromisso com nossos clientes?"

Evidenciada a questão, a resposta era clara. Não podemos entregar os dados dos clientes voluntariamente sem um processo legal válido. E, como advogado sênior da empresa, tenho que assumir a responsabilidade — e enfrentar qualquer crítica — devido à minha posição. Afinal de contas, quem melhor do que os advogados para defender os direitos dos clientes que atendemos?

Nesse contexto, no segundo semestre de 2013, basicamente todas as principais empresas tecnológicas estavam na defensiva. Encaminhamos nossa frustração às autoridades em Washington, D.C. Foi um momento decisivo. As divergências que vieram à tona contribuem até hoje para um abismo entre os governantes e o setor de tecnologia. Os governos servem aos eleitores que vivem em um determinado local, como um estado ou nação. O alcance da tecnologia, no entanto, é global, e nossos clientes estão em praticamente todos os lugares.

A nuvem não somente mudou em que lugar e para quem fornecemos nossos serviços, como também ressignificou nosso relacionamento com os clientes. Ela transformou empresas de tecnologia em instituições que, de certa forma, se assemelham a bancos. As pessoas depositam seu dinheiro em bancos e armazenam suas informações mais pessoais — e-mails, fotos, documentos e mensagens de texto — em empresas tecnológicas.

Esse novo relacionamento também tem consequências que ultrapassam o próprio setor tecnológico. Assim como as autoridades públicas concluíram na década de 1930 que os bancos haviam assumido tamanha importância para que a economia não fosse regulamentada, as empresas tecnológicas se tornaram importantes demais nos dias de hoje para serem deixadas à mercê da abordagem política de *laissez-faire*. Elas precisam se submeter ao Estado de Direito e a uma regulamentação mais ativa. Mas, ao contrário dos bancos dos anos 1930, atualmente as empresas de tecnologia operam em escala mundial, complicando ainda mais a questão da regulamentação.

Em 2013, à medida que a insatisfação dos clientes crescia mundo afora, percebemos que não havia como resolver seus problemas sem dizer nada. Conhecíamos bem os limites inequívocos que havíamos imposto aos nossos próprios serviços, e o trabalho, por vezes complicado, de encarar as práticas preexistentes das empresas que compramos posteriormente. Queríamos explicar que só cedíamos informações de clientes em resposta a mandados de busca e apreensão, intimações e pedidos de segurança nacional. Mas, quando nos propusemos a informar isso publicamente, o Departamento de Justiça, ou DOJ, nos disse que as informações eram sigilosas e não podíamos. A frustração só aumentava.

Decidimos então fazer algo que nunca havíamos feito antes: processar o governo dos Estados Unidos. Para uma empresa que havia resistido a uma década de litígio antitruste do governo e depois passado outra negociando a paz, aparentemente estávamos adentrando em uma nova Cruzada. Entramos com uma petição que inicialmente foi mantida em sigilo no Tribunal de Vigilância da Inteligência Estrangeira dos Estados Unidos, ou FISC.

O FISC é um tribunal especialmente instituído para analisar os pedidos governamentais de vigilância. Foi criado durante a Guerra Fria com o intuito de aprovar escutas telefônicas, coleta eletrônica de dados e monitoramento de suspeitos de terrorismo e espiões. É envolto em sigilo, a fim de proteger as tentativas do serviço secreto de monitorar e frustrar ameaças à segurança. Cada mandado expedido de acordo com a Lei de Vigilância de Inteligência Estrangeira (FISA) acompanha uma ordem de sigilo, que nos

proíbe de informar ao nosso cliente que recebemos um mandado para seus dados. Ainda que isso fosse compreensível, nosso processo judicial alegava que tínhamos o direito de compartilhar informações mais abrangentes com o público nos termos da Primeira Emenda da Constituição e de seu compromisso com a liberdade de expressão. Pelo menos, defendíamos, isso nos facultava o direito de falar de modo geral sobre a quantidade e os tipos de pedidos que recebíamos.

Logo soubemos que o Google havia feito a mesma coisa. Isso resultou em um segundo momento decisivo. Durante cinco anos, lutávamos contra nossas desavenças perante os órgãos reguladores de todo o mundo. O Google defendia restrições no Windows. A Microsoft argumentava em prol de restrições nos mecanismos de busca do Google. Conhecíamo-nos muito bem. Eu respeitava muito Kent Walker, advogado-geral do Google. Mas ninguém nos acusaria de sermos melhores amigos.

De repente, estávamos do mesmo lado, em uma nova disputa em comum contra nosso próprio governo. Decidi me aliar a Kent, a princípio sem sorte, enquanto trocávamos mensagens. Em uma manhã de julho, ao sair de uma reunião aberta com os colaboradores em um dos edifícios onde nossa equipe do Xbox trabalhava, peguei meu celular para tentar entrar em contato novamente. Procurei um canto silencioso e me vi ao lado de um recorte de papelão em tamanho real do Master Chief, o soldado que lidera as tropas em nosso jogo *Halo*, em guerra contra um inimigo alienígena. Apreciei o fato de que o Master Chief estivesse me dando cobertura.

Kent atendeu minha ligação. Embora tivéssemos conversado muitas vezes antes, quase sempre era para discutir as reclamações que nossas empresas tinham umas contra as outras. Agora, eu propunha algo diferente. "Vamos unir forças e ver se conseguimos negociar com o DOJ juntos."

Eu não culparia Kent se ele suspeitasse de um cavalo de Troia. Mas ele ouviu e me retornou um dia depois, dizendo que queria que trabalhássemos juntos.

Fizemos um call com o governo a fim de tentar negociar termos comuns. Parecia que estávamos chegando perto de um acordo, quando, porventura, no final de agosto, as negociações foram por água abaixo. Olhando de nossa posição privilegiada, ao que tudo indicava, a NSA e o FBI não estavam falando a mesma língua. À medida que o verão desaparecia em 2013, as constantes revelações de Snowden erguiam uma barreira ainda mais profunda entre o governo dos EUA e o setor tecnológico. E as coisas foram de mal a pior.

No dia 30 de outubro, o *Washington Post* publicou uma história que deixou o setor em desespero: "NSA Infiltra Links no Yahoo e nos Data Center do Google em Todo o Mundo, Afirmam os Documentos de Snowden."[26] O coautor da história era Bart Gellman, um jornalista que eu conhecia e respeitava, desde que ele escrevia para o jornal *Daily Princetonian,* na Universidade de Princeton, onde éramos estudantes universitários. Seu artigo alegava que a NSA, com a ajuda do governo britânico, acessava secretamente cabos de fibra óptica submarinos para copiar dados das redes Yahoo e Google. Embora não conseguíssemos averiguar se a NSA visava os nossos cabos, alguns dos documentos de Snowden também mencionavam os nossos serviços de e-mail e mensagens do consumidor.[27]

Isso nos fazia suspeitar de que também tínhamos sido grampeados. Até hoje, os governos dos EUA e da Grã-Bretanha não se manifestaram publicamente para negar o hackeamento dos cabos de dados.

O setor tecnológico reagiu com um misto de perplexidade e indignação. Por um lado, a história fornecia o elo perdido acerca de nosso entendimento em relação aos documentos Snowden. Isso sugeria que a NSA tinha acesso a muito mais dados do que fornecíamos legalmente, por meio de ordens de segurança nacional e mandados de busca e apreensão. Se isso fosse verdade, o governo efetivamente estava conduzindo, em grande escala, uma busca e apreensão de informações privadas das pessoas.

A reportagem do *Washington Post* indicava que a NSA, em colaboração com sua contraparte britânica, estava extraindo os dados dos cabos

usados pelas empresas de tecnologia norte-americanas, possivelmente sem controle ou fiscalização judicial. Nossa preocupação era que isso estivesse acontecendo no local em que os cabos se cruzavam no Reino Unido. À medida que os advogados da indústria tecnológica trocavam informações, especulávamos que talvez a NSA tenha se convencido de que, trabalhando ou confiando no governo britânico e intervindo fora das fronteiras dos EUA, ela não estaria sujeita à Quarta Emenda à Constituição dos Estados Unidos e à sua exigência de que a NSA somente poderia buscar e aprender informações conforme as devidas ordens e processos judiciais.

A reação na Microsoft e em todo o setor foi imediata. Nas próximas semanas, nós e outras empresas anunciamos que implementaríamos uma criptografia robusta em todos os dados que movimentávamos entre nossos data centers pelos cabos de fibra óptica, assim como em todos os dados armazenados nos servidores dos próprios data centers.[28] Era uma medida indispensável para proteger nossos clientes, porque significava que, mesmo que um governo desviasse os dados dos clientes na surdina, acessando um cabo, eventualmente não conseguiria desbloquear e ler o que obtivera.

Entretanto, esse tipo de criptografia avançada era mais difícil do que parecia. Envolveria workloads gigantescos para nossos data centers e exigiria um esforço substancial de engenharia. Alguns de nossos líderes tecnológicos não estavam nem um pouco entusiasmados. Os receios eram compreensíveis. O desenvolvimento de software envolve intrinsecamente escolhas entre as funcionalidades, dada a disponibilidade finita de recursos tecnológicos que podem ser implementados em um cronograma viável. Essa criptografia exigia que eles postergassem o desenvolvimento de outras funcionalidades de produtos que os clientes estavam pedindo que acrescentássemos. Após uma discussão acalorada, o CEO Steve Ballmer e nossa equipe de liderança sênior tomaram a decisão de avançar rapidamente na frente da criptografia. Todas as outras empresas de tecnologia fizeram a mesma coisa.

Em novembro daquele ano, à medida que esses acontecimentos se desenrolavam, o presidente Barack Obama visitou Seattle. Ele esta-