

A privacidade está morta. Vida longa à privacidade!



Quase toda tecnologia nova chega com o fardo de matar a privacidade. Mas uma coisa é certeza: leis e regulamentações não são suficientes para manter nossos dados seguros.



AUTOR
**Sherry
Jones**

A cada ano novas manchetes alertam sobre a chegada de uma nova tecnologia específica que chega com a promessa de dar um fim definitivo à privacidade. Mas cenários apocalípticos que preveem a morte da privacidade são quase tão antigos quanto o próprio conceito de privacidade, que na verdade não é tão antigo assim. Neste artigo vamos explorar a relação da sociedade ocidental com a privacidade ao longo do tempo e as implicações dessa relação na era digital.

O sonho da privacidade nasceu em uma cama comunitária

A ideia de privacidade surgiu na Inglaterra no século XIX, como afirma o historiador Georges Duby em sua obra “A história da vida privada” (“A history of private life”, em inglês). A palavra “privacidade” tem sua origem no termo francês “priver”, que significa “domar”, “domesticar”. O termo similar em latim, “privatum”, também se refere ao que acontece dentro de casa ou dentro do círculo familiar.

Na Idade Média, segundo defende Duby, passar tempo sozinho era um privilégio raro. Camas eram extremamente caras e por isso eram compartilhadas por todos da família, exceto nos lares mais abastados. E, ainda que a realeza e os aristocratas tivessem suas próprias camas, os quartos raramente eram ocupados por uma pessoa só: serventes e guardas se mantinham sempre por perto.

Mas compartilhar quartos na hora de dormir não era algo único das sociedades ocidentais. Antropólogos que estudam os nativos das Ilhas Trobriand, uma antiga tribo de caçadores que vive nos arquipélagos da Nova Guiné, reportam que as famílias do grupo viviam e dormiam em cabanas de um quarto só. Quando os pais queriam um momento íntimo, a ordem era para que as crianças cobrissem suas cabeças com tapetes.

Pegando uma cerveja e as correspondências dos outros



A privacidade em termos de correspondência também não era algo muito regular. Até porque um selo de cera não é uma grande garantia de que um envelope vai chegar intacto ao seu destino, com seu conteúdo ainda secreto.

No livro “O direito a privacidade na história estadunidense” (“The right to privacy in American history”, em inglês), o autor David J. Seipp descreve como as cartas chegavam da Inglaterra no século XIX por meio dos navios mercantes.



As correspondências eram entregues nas tavernas e armazenadas numa bolsa com acesso liberado para qualquer pessoa, inclusive para o destinatário.

Até que em 1710 o governo britânico nos Estados Unidos emitiu o “Post Office Act”, que criou um serviço postal regulamentado e tornou proibido o ato de abrir correspondências alheias. E essa se tornou a primeira lei de privacidade estabelecida nos EUA.

Ao criar um serviço postal, o governo tinha como objetivo proteger a privacidade individual de cada um. Mesmo assim, nem todos fizeram questão dela. Por certo tempo, muitas pessoas ainda preferiram a conveniência das entregas via navio mercante, apesar de todos os riscos envolvidos.

Quando os telefones chegaram na festa

Assim como em outros momentos, a chegada dos primeiros telefones aos EUA também geraram previsões calamitosas para a privacidade. E até havia uma boa razão, já que os primeiros telefones ficavam em locais públicos, como lojas e mercados. Ou seja, as pessoas podiam ouvir as conversas alheias enquanto faziam fila para fazer ou receber suas próprias chamadas. As ligações passam ainda por uma central de distribuição, onde as telefonistas faziam as conexões manualmente enquanto ouviam por acaso todas as conversas.

Quando os telefones se tornaram um objeto doméstico muitos deles funcionavam através de linhas coletivas, chamadas em inglês de “party lines”, com diversas casas compartilhando uma só linha. Quando alguém quisesse fazer uma chamada a pessoa era obrigada a tirar o telefone do gancho e verificar se não havia ninguém conversando na linha.

Mas apesar das preocupações sobre privacidade, as pessoas continuaram usando o telefone. Principalmente porque permitia a elas compartilhar informações em tempo real ao invés de mandar caros telegramas ou cartas que demoravam dias, semanas ou até meses para chegar.

Talvez as pessoas estivessem dispostas a sacrificar um pouco da sua privacidade porque confiavam que a tecnologia poderia solucionar os próprios problemas. Com o passar do tempo, as linhas particulares se tornaram cada vez mais acessíveis e as linhas coletivas desapareceram.

Hackeáveis, porém desejáveis

A era digital nos apresentou um conjunto particular de desafios sobre privacidade. A internet, criada para facilitar a troca gratuita e aberta de informações é também o elemento que permite que essas informações sejam usadas de formas não tão agradáveis.

Um exemplo são governos de diferentes partes do mundo, que conduzem programas de “vigilância digital” de seus cidadãos usando tecnologias de reconhecimento facial. Outro caso são os assistentes pessoais, como Alexa (Amazon) e Siri (Apple), Smart TVs e outros aparelhos eletrônicos conectados à internet, que têm se tornado alvo constante dos hackers. Ainda assim, a venda de produtos que utilizam a chamada Internet das Coisas (IoT) não deixa de crescer. Existe até um relatório que prevê que o número de assistentes de voz ativos deve triplicar até 2023 e atingir mais de 8 bilhões.

Protegendo-nos de nós mesmos

Alguns podem dizer que a privacidade está perdendo lugar para a conveniência e o conforto que a Internet fornece. Ao mesmo tempo, muitas pessoas e organizações clamam por regras ainda mais restritas na proteção de dados pessoais.

Governos de todo o planeta estão começando a impor um controle mais duro sobre a coleta, o uso, o compartilhamento e a venda de dados pessoais. As medidas mais destacadas são o GDPR, Regulamento Geral de Proteção de Dados, criado pela União Europeia, e o US State of California's California Consumer Privacy Act, mais conhecido como CCPA, aplicado pela Califórnia.

” Mas enquanto alguns governos aumentam a proteção à privacidade, as pessoas continuam postando informações particulares nas redes.

Muitas delas abrem mão de seus dados pessoais sem nem saber como esses dados serão usados. Mas os vigilantes da privacidade e muitos consumidores ao redor do mundo estão cada vez mais preocupados com o potencial uso dos dados da chamada “Big Tech”, que inclui empresas como Google, Facebook e Apple, para a manipulação política e cultural.

Recentemente, a Comissão Federal de Comércio dos EUA multou o grupo Facebook em incríveis US\$ 5 bilhões por vender dados de seus usuários para a consultoria política Cambridge Analytica. Reportagens indicam que essa empresa usou esses dados para influenciar disputas políticas e eleições em diversos países através das redes sociais.

Vivemos todos num grande Big Brother. Mas será que as pessoas se importam?

A privacidade é algo importante para os consumidores hoje em dia? A resposta depende de quem responderá à pergunta.



Em teoria, os millennials supostamente são aqueles que têm maior indiferença sobre a segurança de seus dados pessoais. Num estudo de 2016 realizado no Reino Unido e nos EUA, 70% dos millennials (entre 19 e 36 anos) afirmaram que acham que sua privacidade online provavelmente já foi ou ainda será comprometida, mas que não se preocupam muito com isso.

No entanto, uma pesquisa mais recente da Internet Innovation Alliance não encontrou diferenças significativas entre o nível de preocupação sobre privacidade de dados dos millennials e de outras gerações.

Em 2019, numa pesquisa da Internet Society com consumidores da Austrália, Canadá, Japão, França, RU e EUA, 75% dos entrevistados mostraram certa preocupação com o fato de que as empresas compartilhem seus dados pessoais sem seu consentimento. Um número ainda maior, 88%, quer que os governos garantam seu direito à privacidade de dados, enquanto 80% acredita que as leis e regulamentações atuais não são suficientes.

E eles estão certos.

Vivemos todos num grande Big Brother. Mas será que as pessoas se importam?

A história mostra que a tecnologia e a engenhosidade humana combinadas podem, muitas vezes, solucionar os problemas que elas mesmas criaram.

Quando as pessoas postam seus próprios dados pessoais nas redes sociais, elas estão escolhendo fazer isso. As violações ocorrem quando aquela rede social ou outros sites vendem ou compartilham esses dados sem o consentimento do usuário. Mas uma internet aberta e livre não significa que você precise compartilhar seus dados mais sensíveis.

Leis podem ajudar-nos, mas infelizmente elas só chegam até certo ponto. E a realidade é que os legisladores ainda estão começando a entender quais são as melhores maneiras de impor restrições na coleta e uso de dados sem ferir o livre comércio.

A verdade é que a privacidade tem uma luz no fim do túnel, e essa luz é a inovação. Em resposta aos riscos crescentes relacionados à coleta e uso de dados pessoais, as empresas de tecnologia estão começando a criar alternativas para seus usuários para que estes escolham manter seus dados privados ou não.

O mecanismo de busca DuckDuckGo, por exemplo, não guarda o histórico de busca dos usuários e nem seus dados. Alguns serviços de adblock também fazem o mesmo.

A rede social MeWe é outra que fornece aos usuários uma Declaração de Direitos de Privacidade, na qual promete que as informações fornecidas pertencem somente ao usuário e que o site nunca irá vendê-las ou compartilhá-las.

No mundo dos negócios, a startup Duality Technologies inventou a “criptação homomórfica”, que permite que empresas de tecnologia analisem dados pessoais criptografados sem precisar remover a criptografia. Segundo informações, o Google agora também passou a fornecer uma ferramenta de criptação homomórfica para seus parceiros.

Tecnologias emergentes também prometem melhorar a privacidade. O Blockchain é uma tecnologia que é a base para o Bitcoin e outras moedas digitais, e funciona linkando transações através de um livro-razão ou livro contábil distribuído, visível para múltiplos usuários e imutável. Alguns especialistas preveem que o Blockchain também será utilizado para criar novos formatos de identidade digital criptografados.

Um startup chamada Polys, por exemplo, está usando uma combinação de criptografia e Blockchain para tornar **votações online anônimas e ao mesmo tempo verificáveis**, assegurando a proteção aos eleitores e também a segurança dos resultados.

A triste realidade é que algumas (ou muitas) empresas de tecnologia e líderes de empresas não vão ter o interesse público como uma de suas prioridades. Esse é um dos motivos pelos quais precisamos de leis e regulamentações para resguardar a privacidade. Mas até mesmo os consumidores sabem que os governantes não têm como ter controle sobre tudo.

Uma nova era da privacidade está começando. O que as empresas devem fazer?

A luta pela privacidade de dados precisa de regras mais duras. Mas o problema é que, se essas regras forem duras demais, podemos inibir a inovação.

O melhor remédio é a combinação dessas duas coisas: leis de privacidade flexíveis e ferramentas digitais que permitam que os usuários protejam seus dados. Essa combinação reforçada dará início a uma nova era em que nossas informações serão tão privadas quanto seus proprietários desejem.

Para se preparar para essa nova era focada na privacidade, as organizações devem começar a se planejar agora para resguardar os dados que elas manipulam, seguindo os parâmetros de regulamentação da GDPR e da CCPA, mesmo que essas leis não se apliquem ao seu país ou organização. Você também deve assegurar que seus parceiros operacionais façam o mesmo. Usar tecnologias para privacidade de dados ou inventar sua própria tecnologia também são coisas que devem fazer parte desse processo.

Em seguida, sua empresa deve divulgar seu compromisso com a privacidade de dados, por exemplo, publicando uma “declaração de direitos de privacidade”, como outros fizeram.

” Se estabelecer como um líder do movimento a favor da privacidade de dados pode ajudar a melhorar o perfil da sua empresa e deixá-la um patamar acima dos competidores.

Pessoas físicas podem apostar na ingenuidade humana, mas os negócios não. As empresas precisam fazer seu papel: priorizar o direito à privacidade de seus consumidores e fornecer acesso fácil a serviços que colaborem para a proteção dos mesmos.

A inovação pode, e deve, abrir o caminho para o renascimento da privacidade, dando aos indivíduos e às empresas um controle sem precedentes sobre seus dados. E, enquanto isso, a era digital vai continuar enriquecendo nossas vidas de diversas maneiras.

Este é um artigo opinativo e não necessariamente reflete as opiniões e posicionamentos da Kaspersky.



O REAL VALOR DA PRIVACIDADE DIGITAL

Pesquisamos as atitudes e expectativas de 11.000 consumidores em todo o mundo em relação à privacidade de dados.

[LEIA O RELATÓRIO](#)