

# Quem vê o seu perfil?



Shutterstock/Montagem Ideac

Analizamos as políticas de privacidade e os termos de uso do Facebook, Google+ e Twitter para saber o que eles dizem fazer com as informações pessoais dos usuários

**M**ostrar fotos de uma viagem ou do seu bichinho de estimação; dar a sua opinião sobre o cenário político ou sobre o último jogo do seu time de futebol; compartilhar vídeos engraçados ou campanhas contra a violência. Tudo isso é possível nas redes sociais, e talvez esse seja um dos segredos de seu sucesso. Segundo uma pesquisa realizada pelo Ibope em setembro de 2010, 20% dos brasileiros já utilizavam esses sites àquela época. Atualmente, só o Facebook tem 63 milhões de usuários cadastrados no país, de acordo com o site Socialbakers. O desejo de compartilhar aquilo que pensamos e fazemos com um extenso grupo de amigos e conhecidos e, ao mesmo tempo, saber o que eles fazem e pensam é o grande atrativo das redes sociais. Mas você, usuário, já se perguntou o que a empresa faz com as suas informações pessoais?

Para tentar descobrir essa resposta, o Idec analisou as políticas de privacidade e os termos de uso de três importantes redes sociais: Facebook, Google+ e Twitter. “O objetivo foi averiguar o que as empresas declaram garantir em relação à privacidade dos usuários. Se elas têm cumprido ou não o que informam em suas políticas só será possível afirmar na segunda parte da pesquisa, que deve ser publicada no primeiro semestre de 2013”, informa Guilherme Varella, advogado do Idec responsável pelo levantamento.

A primeira constatação é de que as redes sociais sabem muito sobre a vida dos usuários. A quantidade de informações recolhidas é enorme, em especial no Facebook e no Google+. Praticamente tudo o que é fornecido na hora de criar a conta ou durante a utilização do serviço (como postagens, compartilhamentos, contatos, comentários etc.) é registrado e pode ser utilizado, segundo as políticas de privacidade. “A questão é: a empresa precisa de todas essas informações? Aparentemente, a quantidade de dados recolhidos é desproporcional ao que ela necessita para prestar o serviço”, aponta Varella.

Além dos dados obtidos na rede social, no caso do Google, principalmente, existe a possibilidade de cruzamento de informações entre serviços da mesma empresa, como o conteúdo de e-mails, os vídeos postados e assistidos (o Youtube pertence ao Google) e até as informações pesquisadas, caso o usuário acesse o serviço de busca enquanto estiver logado à rede social ou à sua

conta no Gmail. “Com isso, a empresa sabe absolutamente tudo sobre a vida de milhões de usuários, formando um banco de dados extremamente qualificado, e não há garantias de que ele não será negociado com terceiros”, alerta o advogado do Idec. “A rede social sabe mais do cidadão que ele mesmo, e forma perfis a partir dessas informações. Essa condição é óbvia para as empresas, mas não está nada clara para os internautas”, completa Luiz Costa, procurador do Ministério Público Federal em São Paulo (MPF) e especialista em privacidade.

Uma enquete realizada pelo Idec durante o mês de novembro indica que a grande maioria dos internautas que participa de redes sociais não conhece as regras do jogo: 84% disseram não ter lido os termos de privacidade dos sites de que participam. “Qual a legitimidade dessas condições para as quais o usuário diz ‘sim’ sem ler?”, questiona Costa.

## MERCADO DE DADOS

As três redes sociais se comprometem, em sua política de privacidade, a não vender os dados pessoais dos usuários a terceiros. No entanto, todas afirmam que os utilizam para oferecer “melhoria nos serviços, publicidade relevante e conteúdo personalizado”. “Oficialmente, as empresas fazem publicidade direcionada, de acordo com os interesses dos usuários, a partir das páginas que ele curte na

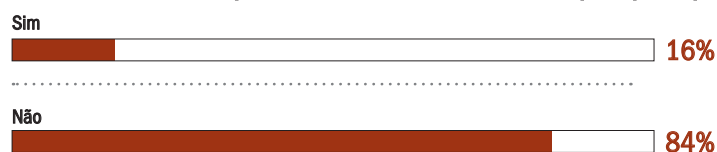
## COMO FOI FEITA A PESQUISA

Entre os dias 15 e 30 de outubro, o Idec avaliou as informações disponíveis nas políticas de privacidade e nos termos de uso das redes sociais Facebook, Google+ e Twitter. A análise levou em conta padrões internacionais de proteção da privacidade, a legislação nacional, como o Código de Defesa do Consumidor, e os princípios de proteção de dados pessoais previstos no anteprojeto de lei elaborado pelo Ministério da Justiça.

O resultado do levantamento foi enviado às três empresas, mas nenhuma delas se manifestou.

### ENQUETE

**De 1º a 28 de novembro, disponibilizamos em nosso portal a pergunta: você leu os termos de privacidade das redes sociais das quais participa?**



470 internautas votaram

rede social, dos anúncios em que clica etc. É difícil saber se elas vendem ou não os dados a outras empresas. Mas é fato que o banco de dados com informações pessoais dos usuários é muito valioso, financeiramente falando”, afirma Tulio Vianna, professor da Universidade Federal de Minas Gerais (UFMG) e especialista em Direito Penal na internet.

Considerando-se que as redes sociais são gratuitas, é de se imaginar que o usuário “pague” o serviço de alguma forma. Ao que tudo indica, a moeda, nesse caso, são as suas informações pessoais e os seus hábitos de consumo. “Quando se cadastra na rede social, o internauta autoriza, automaticamente, o recebimento de publicidade. Porém, as políticas de privacidade não informam claramente que a cada vez que a rede é utilizada, são gerados dados que servirão de insumo para futuros anúncios publicitários. Isso precisa ficar mais claro”, ressalta Varella.

As empresas dão ao usuário a possibilidade de configuração das contas para reduzir o envio de anúncios e conteúdos personalizados. Porém, destacam que, se ele optar pelo

modelo de “mínima publicidade”, as funcionalidades dos serviços oferecidos podem ser reduzidas. Vale ressaltar que, na maioria dos casos, a configuração padrão das contas na rede social é a mais “aberta” possível, permitindo amplo acesso aos dados do usuário. Para não ficar tão exposto, é preciso alterar a configuração padrão, “desmarcando” os itens que autorizam o acesso e o uso das informações. Essa prática é chamada de *opt-out*, pois o usuário precisa “optar por sair”. “O ideal é que fosse o contrário, que o padrão fosse mais rigoroso do ponto de vista da proteção à privacidade, e que houvesse a opção de tornar a conta mais ‘aberta’”, defende o advogado do Idec.

Além disso, por mais que a conta possa ser cancelada nas três redes sociais, não há garantias de que as informações dos usuários

### Número de usuários no Brasil em 2012



Facebook  
**63**  
milhões



Twitter  
**33,3**  
milhões



Google+  
**7,5**  
milhões

Fonte: sites Socialbakers e SemioCast

Resultado da pesquisa			
	Facebook	Google+	Twitter
A política de privacidade é acessível?	Sim. Fácil de encontrar na página, linguagem simples, texto em português		
Permite configurar a privacidade e reduzir o envio de anúncios personalizados?	Mais ou menos. Não garante o pleno funcionamento do serviço caso o usuário altere a configuração		
Tem canais para reclamações e dúvidas?	Mais ou menos. Há formulário em português, fácil de ser encontrado, porém, exibe endereço americano para correspondência e não tem telefone de contato		
Responsabiliza-se pela prestação dos serviços?	Não. Exime-se de responsabilidade, tenta reduzir o direito à indenização do consumidor e baseia seus termos nas leis norte-americanas		
A quantidade de dados pessoais utilizada é grande?	Sim. Praticamente todas as informações são utilizadas pela empresa	Sim. O cruzamento dos diversos serviços oferecidos pela empresa aumenta o nível de utilização dos dados	Mais ou menos. Pela natureza da rede, são exigidas menos informações
Informa para que os dados serão utilizados?	Mais ou menos. Diz apenas que utiliza os dados pessoais para aprimorar os serviços e fornecer anúncios relevantes	Sim	Mais ou menos. Diz apenas que utiliza os dados pessoais para aprimorar os serviços e fornecer anúncios relevantes
Transfere dados pessoais a terceiros?	Sim. Repassa os dados aos afiliados*, parceiros comerciais, provedores e empresas terceirizadas, a menos que o usuário desative todos os aplicativos	Mais ou menos. A empresa afirma que só transfere com autorização do usuário, que é automática. O consumidor precisa desautorizar ( <i>opt-out</i> )	Mais ou menos. A empresa afirma que só transfere informações com autorização do consumidor, mas não se sabe exatamente como isso se dá
A empresa permanece com os dados do usuário após o cancelamento da conta?	Sim. Fica com informações por mais 90 dias depois do cancelamento	Sim. Os dados removidos pelo usuário não são excluídos automaticamente e podem permanecer como backup da empresa	Não há informações sobre isso

\*Afiliados são acionistas que fazem parte do grupo que comanda o Facebook, agora que a empresa abriu seu capital

serão realmente excluídas do banco de dados da empresa, ou se só não ficarão mais visíveis. Veja na tabela na página anterior um resumo dos principais resultados da pesquisa.

### SEM LEI

A falta de transparência sobre o que é feito com as informações dos usuários ocorre principalmente porque não há no Brasil uma lei que assegure a proteção de dados pessoais. Em 2010, o Ministério da Justiça (MJ) começou a elaborar um anteprojeto de lei sobre o assunto, que foi posto em consulta pública, mas ainda não foi consolidado pela pasta. De acordo com Danilo Doneda, coordenador-geral de supervisão e controle do Departamento de Proteção e Defesa do Consumidor (DPDC), o anteprojeto deve ser enviado muito em breve (talvez ainda este ano) à Casa Civil e, de lá, ao Congresso, onde passará por votação para, depois, ir à sanção presidencial.

Para o professor Tulio Vianna, a aprovação de uma lei que regulamente a proteção de dados é fundamental, pois determinaria quais informações podem ser coletadas e restringiria

claramente o que pode ser feito com o banco de dados – e essas regras não seriam só para as redes sociais, mas para todas as empresas que lidam com dados pessoais. “A Lei de Proteção de Dados representaria para a sociedade da informação o que o Código de Defesa do Consumidor representa para a sociedade de bens e serviços”, compara Luiz Costa, do MPF.

O advogado do Idec explica que, com uma legislação específica, as empresas teriam de seguir alguns princípios legais, como o da proporcionalidade (só pedir dados que realmente sejam necessários para prestar o serviço); da finalidade (informar o que vão fazer com as informações coletadas) e da autodeterminação (que garante que os dados só serão usados com autorização expressa do consumidor).

## Os riscos de se expor

No dia a dia, a questão da privacidade nas redes sociais é lembrada mais pela possibilidade de exposição da intimidade a pessoas que não gostaríamos que soubessem de nossa vida. E esse risco realmente existe. “Quando publica algo numa rede social, o usuário deve considerar que está num lugar público, e que tudo que é divulgado pode ser lido ou acessado por qualquer pessoa”, ressalta Miriam von Zuben, analista de segurança do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), do Comitê Gestor da Internet no Brasil (CGI.br).

Tulio Vianna, da UFMG, destaca o perigo de os dados divulgados na rede serem usados por criminosos. Por exemplo, avisar na rede que vai viajar com a família toda (ou publicar fotos enquanto está fora) significa anunciar que a casa estará vazia, um alvo fácil para furto. O mesmo vale para ferramentas de “check-in” (quando o usuário informa onde está). “As pessoas se expõem acreditando na boa-fé dos outros e que a informação será vista apenas por seus amigos, mas o risco é muito mais amplo”, adverte Vianna.

O professor também comenta sobre o problema de expor dados pessoais “sensíveis”, como orientação sexual e religiosa. Por mais que o Brasil seja, em tese, um país tolerante, não dá para descartar a possibilidade de essas informações serem capturadas por grupos intolerantes. Para Vianna, informações sensíveis não devem ser questionadas no cadastro de redes sociais.

Há ainda uma série de outros riscos, como roubo de identidade – os dados de um perfil ou mesmo fotos podem ser copiados e utilizados em outros sites – ou criação de perfil falso. “Quanto

mais informações o usuário divulga sobre si, mais convincente o perfil falso será, e maiores serão as chances de os amigos acreditarem que a página é verdadeira”, alerta Miriam. ■

### Como proteger sua privacidade

- **Configure a privacidade de sua conta da forma mais restritiva possível.** Algumas opções costumam vir, por padrão, definidas como públicas, mas podem ser alteradas.
- **Mantenha o seu perfil privado**, permitindo o acesso somente a pessoas ou grupos específicos.
- **Só aceite convites de pessoas que realmente conheça.**
- **Cuidado ao aceitar aplicativos e jogos.** Por meio deles, suas informações pessoais podem ser acessadas, por exemplo, por grupos de pessoas intolerantes e até por criminosos.



#### SAIBA MAIS

Cartilha de Segurança para Internet do CERT.Br <<http://goo.gl/qwbT5>>