Breno Rios

Introdução à Ciência dos Dados - Exercício 3

25 de Outubro de 2018

Desafios e possíveis soluções para a proteção da privacidade

Lei, tecnologia e/ou mercado?

Introdução

A quantidade de dados gerada nos últimos tempos tem crescido exponencialmente. Esse crescimento traz desafios relacionados a proteção da privacidade para governos, empresas e usuários. Esses desafios vem de diferentes perspectivas. Há desafios e soluções tecnológicas a serem discutidos e desafios em relação a leis efetivas em favor da proteção da privacidade, e talvez o mais importante e, em minha opinião, mais eficazes quando resolvidos: desafios em relação a incentivos de mercado para a proteção da privacidade.

Nas seções subsequentes, vamos navegar por alguns desses desafios e por possíveis soluções dadas pelos autores dos seguintes artigos: *Control use of data to protect privacy (Susan Landau), What the "right to be forgotten" means for privacy in a digital age (Abraham L. Newman)* e *Inverse Privacy (Yuri Gurevich, Efim Hudis, and Jeannette M. Wing)*.

Controle de uso de dados

No artigo *Control use of data to protect privacy,* escrito pela especialista em segurança cibernética Susan Landau, ela advoga que os princípios utilizados para a proteção de privacidade não são mais suficientes em nossa era. Os dois princípios são: aviso prévio e consentimento.
Segundo a autora, esses dois princípios acabam perdendo o sentido nos dias de hoje pois, em situações onde a coleta de dados consiste de vários pequenos blocos de informação, o número de decisões a serem feitas, ou ainda, o número de permissões a serem solicitadas seriam extremamente grandes. A autora sugere que o controle do uso é uma alternativa mais eficaz ao controle da coleta de dados.

O artigo começa reconhecendo a importância e alguns dilemas da coleta de dados. Um cenário que exemplifica um desses dilemas é o de, no caso de um acidente que bloqueie o tráfego em uma rota principal, a coleta de dados de localização deveria aumentar para prover um melhor serviço para os usuários da plataforma? E se alguns desses usuários estiverem em um modo privado

naquele dia, ou seja, não estão permitindo a coleta de dados? Se a coleta for cessada, a qualidade do serviço cai. Já se a coleta constante, mesmo com constantes avisos prévios, que segundo ela, levam ao usuário sempre clicar "Sim" inadvertidamente, prejudica a proteção da privacidade.

A solução principal dada pela autora é o controle do uso. Um dos exemplos citados é o protocolo criado por pesquisadores do MIT, chamado httpa (accountable http). O protocolo transmite restrições de uso entre provedores de dados e usuários desses dados, e cria um log em uma PTN (Provenance Tracking Network) toda vez que um recurso protegido é acessado. Essa técnica não consegue impor conformidade, mas consegue determinar se ela foi alcançada.

O direito de ser esquecido: local e globalmente

No artigo *What the "right to be forgotten" means for privacy in a digital age,* escrito pelo professor associado da Universidade de Georgetown, Abraham L. Newman, o foco é no "direito de ser esquecido", criado pela Corte de Justiça Européia em maio de 2014. Isso significa que qualquer cidadão europeu pode requerir que mecanismos de busca retirem do ar resultados de busca que são falsos, irrelevantes e/ou inacessíveis.

O autor combate algumas principais objeções a essa lei. Uma delas é o argumento de que as empresas iriam ser enterradas em custos por causa do processamento desses pedidos, e ainda que os requerentes estariam infringindo a liberdade de expressão alterando resultados de buscas. A isso, ele responde mostrando a alta do valor de mercado no Google, perto dos 366 bilhões em Dezembro de 2014, e o pequeno número de 180.000 requisições processadas, argumentando que essa lei não iria afundar as finanças das empresas. Em relação a prejudicar a liberdade de expressão, ele usa a própria lei para desbancar isso, dado que a decisão não requere a retirada do conteúdo original, apenas a retirada do aparecimento desse conteúdo nos mecanismos de busca.

Em conclusão, o autor defende o modelo Europeu de garantia de privacidade, mas que ele só teria um efeito completo se além de ter surgido localmente, fosse reforçado globalmente, pois o pedido de retirada acaba sendo executado apenas para domínios locais, mas o conteúdo continua em outros domínios.

Privacidade inversa: incentivo de mercado para garantir a privacidade

No artigo *Inverse Privacy,* com autoria compartilhada entre Yuri Gurevich, Efim Hudis, ligados a Microsoft, e a professora da Universidade de Columbia, Jeannette M. Wing, o foco é buscar soluções de mercado para solucionar o problema de inacessibilidade a informação privada por parte do próprio usuário.

Os autores defendem que, além do óbvio benefício gerado pela coleta de dados pelas empresas, que é servir melhor seu cliente e consequentemente aumentar seus lucros, haveria benefícios na liberação desses dados para os usuários que os geraram. O termo usado por eles para designar esse acesso unilateral a dados privados é privacidade inversa. Também derrubam a objeção de que seria perigoso para a privacidade de outras partes essa liberação mesmo que ela fosse individual, argumentando que, em vários cenários, esse perigo gerado pela liberação é irrisório.

Para se alcançar a diminuição da privacidade inversa, os autores buscam argumentar que há incentivos de mercado para isso. Sendo assim a liberação desses dados para seus usuários geraria valor para o negócio. Algumas pesquisas entre usuários apresentadas no artigo, mostram que a maioria dos usuários gostariam de ter acesso a seus próprios dados, e além disso ter o poder de editá-los para corrigir possíveis erros. Dado essa preferência, esses usuários prefeririam lhe dar com empresas que lhe dessem esse tipo de poder. Além disso, o poder de editar possíveis erros nos dados, ajudaria a melhorar a qualidade dos mesmos, o que serviria para a empresa melhorar seus serviços.

Qual abordagem é mais eficaz?

Muitas vezes, uma mistura de abordagens oferece a melhor solução para um dado problema. Em minha opinião, no problema da proteção da privacidade não seria diferente. Apesar desse pensamento, creio que há uma gradação na eficácia das soluções. A meu ver, a solução mais eficaz é a defendida no artigo *Inverse Privacy*. Se houver valor para os negócios, ou seja, houver algum incentivo de mercado para que a proteção a privacidade e acesso a seus próprios dados privados sejam reforçadas pelas empresas, as soluções tecnológicas defendidas no artigo *Control use of data to protect privacy* irão ser melhoradas e ganharão várias concorrentes em uma velocidade muito maior do que a aprovação de uma lei, defendida no artigo *What the "right to be forgotten" means for privacy in a digital age* poderia fazer por essa causa.

Em vários casos a vontade política, mesmo as que tem um belo discurso em defesa de uma causa bela e moral, acaba causando efeitos colaterais e distorções indesejadas no mercado que acabam prejudicando o mais interessado nisso: o usuário. Os processos de mercado geram soluções melhores e mais efetivas que surgem gradativamente e de acordo com as expectativas dos clientes, exatamente o contrário do que geralmente "canetadas" políticas geram.