E por que ela é tão importante em mercados altamente regulados?

Por Gustavo Artese (*)

À primeira vista, pode parecer que normas de proteção à privacidade de dados pessoais têm como único objetivo evitar que o uso e divulgação de dados pessoais tragam prejuízo a seus titulares (e.g. discriminação, estigmatização). Não é só isso. Além de proteger os titulares da informação, a regulação em privacidade deve permitir também, o tanto quanto possível, o livre fluxo de informações. É uma ciência de equilíbrio.

Com esses objetivos em foco, as leis e regulamentos existentes de proteção à privacidade de dados pessoais categorizam dados pessoais com a finalidade de conferir-lhes grau adequado de proteção (sem restringir demasiadamente o fluxo de dados). Em outras palavras, dados pessoais são categorizados para fins de promoção de uma governança adequada para sua utilização. Nesse sentido, as Privacy Guidelines da OCDE1 reconhecem que “a aplicação de diferentes medidas de proteção para diferentes categorias de dados pessoais, dependendo de sua natureza e o contexto em que são coletados, armazenados, processados ou disseminados”, é costumeira

A esta aplicação de medidas e graus de proteção diferentes para situações diferentes se dá o nome de “**Privacidade em Contexto**”.

As categorizações mais comuns referem-se à:

1 - Sensibilidade dos dados pessoais (e.g. dados relativos à saúde, biometria, genética, opiniões políticas, que revelem origem racial);

2 - O sujeito a quem se referem os dados (e.g. dados associados a menores de idade, empregados ou pacientes);

3 - O propósito para o qual os dados são utilizados (e.g. uso comercial, uso pessoal, investigação policial, propósitos científicos);

4 - O contexto (strictu sensu) no qual os dados são processados (e.g. no contexto de comunicações eletrônicas; criação e guarda de arquivos);

5 - O grau de anonimização dos dados pessoais (e.g. identificador, de-identificado, anônimo, pseudônimo); e

6 - Se o dado foi coletado direta ou indiretamente (para fins de obtenção de consentimento ou dever de notificação).

A consequência prática mais importante da “**Privacidade em Contexto**” é que, uma vez que a regulação depende de contexto, cada atividade econômica (e profissional) que se utilize de dados pessoais na condução de seus negócios estará sujeita a tratamentos regulatórios distintos. Nesse sentido, é natural e esperado, por exemplo, que o tratamento de dados pessoais feito por uma seguradora receba, *ceteris paribus*, tratamento regulatório diferente daquele dispensado a negócio baseado em e-commerce.

Dentre outros motivos, é também em razão da “**Privacidade em Contexto**” que os maiores especialistas sobre o tema defendem que a tutela da privacidade dos dados pessoais empregue “estratégia jurídica” que mescle legislação geral baseada em princípios com normas específicas e/ou códigos de deontologia.

Na área de saúde, a necessidade de se dar tratamento regulatório específico é notável. Não por acaso, os EUA decidiram promulgar lei específica de proteção aos dados pessoais relacionados à saúde do indivíduo.

Não poderia ser diferente. São muitos os motivos para que a área de saúde mereça regras de governança especiais. Dentre esses, destacam-se: (**1**) o fato de que dados pessoais de saúde são extremamente sensíveis; (**2**) para permitir tratamento adequado ao paciente, dados pessoais de saúde devem estar disponíveis de forma livre e indiscriminada aos profissionais de saúde envolvidos; (**3**) o número de profissionais de saúde envolvidos no atendimento a um mesmo indivíduo tende a aumentar (o que, necessariamente, aumenta as chances de quebra de sigilo); (**4**) o emprego especialmente intensivo da tecnologia da informação na área de saúde (e.g. prontuários eletrônicos e uso de dispositivos móveis); e (**5**) o interesse público na utilização de dados pessoais de saúde para finalidades secundárias (e.g. pesquisas médicas).

No Brasil, o direito à privacidade em saúde é tutelado, apenas incidentalmente, por normas de conduta profissional emitidas pelo Conselho Federal de Medicina.

Quando somadas à regra geral, ainda incompleta, trazida pelo Marco Civil da Internet, nos vemos diante de marco regulatório razoavelmente adequado no que respeita à sua estrutura e absolutamente insuficiente no que tange ao seu conteúdo.

O momento atual é de claro incentivo aos investimentos na interoperabilidade dos sistemas de informática na saúde. Como consequência, testemunharemos aumento exponencial no fluxo e disponibilidade de informações e dados associados à saúde do indivíduo.

O livre fluxo de informações pessoais de saúde tem, a um só tempo, o poder de salvar e de prejudicar vidas. Não investir na definição de regulamentação sobre o tema da privacidade no contexto da saúde, tanto contribui para a formação de ambiente de insegurança jurídica, quanto deixa aberta a porta para a perda de confiança no sistema de saúde e em seus agentes.

(*) Gustavo Artese é Master of Laws (LL.M.) pela Universidade de Chicago e Líder das Práticas de Direito Digital, Privacidade e Propriedade Intelectual do escritório Vella Pugliese Buosi e Guidoni Advogados

Fonte: CIO, em 11.08.2014.