Por Gisele Truzzi (*)

Como o GDPR, a legislação da União Europeia que está impactando centenas de empresas de tecnologia, influencia as empresas brasileiras

O **GDPR – General Data Protection Regulation** (Regulamento Geral de Proteção de Dados), é a mais nova legislação que visa fortalecer a proteção de dados pessoais de cidadãos na União Europeia. Ela entrará em vigor no dia 25 de maio de 2018.

De modo geral, a nova lei se aplica a todos aqueles que comercializam bens e serviços junto aos países membros da União Europeia. Seja de forma gratuita ou não. Na prática, esta nova legislação afetará todas as organizações sediadas na Europa ou em outros territórios, mas que atuam também em solo europeu. Ou seja, qualquer empresa que tenha negócios por lá, também precisará se adequar.

Portanto, as empresas brasileiras (privadas ou públicas), mesmo que sediadas em território nacional, caso tenham clientes na Europa, ou até parceiros europeus, terão que atender a tal legislação.

E não importa se sua empresa é uma pequena plataforma de comércio eletrônico ou se é uma multinacional. Se entre as atividades desenvolvidas está a captação e armazenamento de dados dos usuários (e se, por acaso, possam estar cidadãos europeus envolvidos), você deverá atentar-se às novas regras do GDPR.

Além disso, é importante frisar que se sua empresa utiliza serviços dos “gigantes da internet”, tais como Google, Amazon ou Facebook, não adianta responsabilizar tais organizações em caso de desconformidade com o GDPR. Ou seja: não há como alegar desconhecimento da lei ou tentar jogar a responsabilidade para terceiros detentores das plataformas que sua empresa utiliza.

Por isso, é melhor ficar atento aos próximos parágrafos.

Principais mudanças e direitos dos usuários

Uma das grandes obrigações impostas às empresas pelo GDPR é a obtenção de “consentimento expresso e específico” do usuário para fornecimento de determinadas informações. Aqui, estamos falando de dados pessoais e dados “sensíveis”. Entendem-se dados pessoais informações que permitem a identificação ou individualização do usuário, tais como nome, endereço, telefone, número de um documento, fotos, etc. Por sua vez, compreendem-se dados sensíveis aqueles relacionados à saúde, orientação sexual, religião, gostos e interesses pessoais do indivíduo.

Sendo assim, nenhuma empresa pode capturar dados pessoais ou sensíveis dos usuários se estes não fornecerem consentimento expresso para isso. Ou seja, o usuário deverá ser informado exatamente sobre quais dados a empresa coletará e poderá decidir se consente com tal situação ou não. E nesse caso, não adianta apenas revisar os Termos de Uso e Políticas de Privacidade, para abranger as novas regras. Para ser clara: não bastará somente criar um novo “checkbox” a ser preenchido.

Os usuários devem ter a possibilidade de fazer download dos seus dados, exigir sua correção ou exclusão definitiva pelas empresas. Isso significa dizer que cada usuário poderá, por exemplo, solicitar sua *playlist* ao Spotify para tocá-la também no aplicativo concorrente, ou fazer *backup* de todas as suas fotos do Instagram.

O usuário ganha o direito de saber quais informações as empresas detêm e requerer sua exclusão. Isso vale também para bancos, *e-commerce* ou qualquer entidade (pública ou privada) que armazene suas informações.

Recentemente, grandes empresas da internet já estão enviando e-mails automáticos aos usuários informando sobre as principais mudanças que serão implantadas em seus serviços.

Isso permitirá, em tese, uma maior transparência no uso de nossas informações. Outros objetivos são permitir o controle sobre os dados disponibilizados e mobilidade aos usuários.

Essas são as novas obrigações. E quem não cumpri-las, pode sofrer sansões bem duras. O GDPR fixa multas altas em caso de descumprimento. As empresas podem ser multadas em até 4% da sua receita global. O Facebook, por exemplo, poderia ser multado em até US$ 1,6 bilhão.

Por isso há grande preocupação em atender aos principais itens dessa nova lei.

Impactos para os negócios no Brasil

Toda empresa brasileira que venda bens ou serviços com foco na Europa ou cujo público-alvo seja o europeu, deverá se preocupar em atender estritamente as novas regras.

Basicamente, toda operação de coleta, tratamento ou armazenamento de dados deverá atender as novas determinações. Que fique claro: não importa o tamanho da empresa, o volume de dados, ou se a relação desenvolvida com os usuários é gratuita.

É essencial que a empresa faça uma revisão do processamento de dados, a fim de verificar se cada etapa deste procedimento atende às novas determinações. É importante também que se designe um colaborador específico ou consultor externo para atender às requisições relacionadas à privacidade de dados que poderão surgir. Revisar os Termos de Uso e as Políticas de Privacidade é igualmente importante.

O que esperar

Ainda é cedo para saber o que virá após o início da vigência do GDPR.

Na prática, as relações entre usuários e empresas não deverão mudar muito do ponto de vista do usuário, que geralmente não se atenta às inovações inseridas nos documentos das plataformas que utiliza.

Já do ponto de vista das empresas, estas sim deverão fazer a lição de casa e se adequar às novas regras, tendo em vista que seu nível de *compliance* irá aumentar significativamente.

Mas, o mais importante é a mentalidade trazida por esta nova legislação. Há uma nova e maior preocupação com a privacidade dos dados. Com o avanço da tecnologia e facilidade na troca de informações, essa preocupação vinha sendo diminuída.

Só o tempo dirá se continuaremos negociando nossa privacidade e nossos dados em troca de serviços, bens ou produtos, ou se de fato tomaremos as rédeas do que é nosso, por direito.

E no Brasil? Estão fazendo alguma coisa?

Em artigo anterior, mencionei o cenário da nossa legislação nacional sobre o tema “privacidade e proteção de dados pessoais”.

Nosso ordenamento jurídico é bem esparso sobre o assunto e ainda não possuímos uma legislação específica sobre o tema.

Nesse contexto, além do Projeto de Lei 5276 que citei no texto passado, no início deste mês entrou na pauta do Senado Federal o PLS (Projeto de Lei do Senado) nº 330/2013, que visa criar uma lei geral de proteção de dados no nosso país. Entre as disposições do PLS 330/2013 que mais assustaram os especialistas, uma delas era a de que o cumprimento de obrigações relacionadas à

captura, tratamento e armazenamento de dados pelas empresas não se impunha ao Estado. Ou seja: o Estado era excluído do tratamento de dados dos cidadãos. Qualquer semelhança com o "Grande Irmão" de Orwell é mera coincidência. Ou não.

Felizmente, houve uma mudança na redação que diminui tal poder do Estado.

Nesse novo texto, há prazos para armazenamento de dados pessoais por empresas privadas, em contrapartida, há permissão para manter dados de pessoas jurídicas de direito público pela eternidade, para fins científicos, entre outras particularidades.

Mas o que nos assusta é que, diferentemente do GDPR, não foram mencionados os direitos fundamentais para o dono dos dados pessoais: o cidadão. Parece que ele não possui poder sobre seus dados quando estes forem tratados pelo Poder Público. Nossa esperança é que, após o pedido de vista requisitado por alguns senadores, tal redação possa ser aprimorada, e conceda ao cidadão brasileiro o poder que o cidadão europeu terá sobre suas informações, independentemente de a relação ser na esfera privada ou na estatal.

(*) **Gisele Truzzi** é advogada especialista em Direito Digital e fundadora da Truzzi Advogados.

Fonte: Artigo publicado originalmente na revista IstoÉ Dinheiro em 15/05/2018.