Victor Gonçalves: A regulamentação europeia do uso de dados pessoais

As novas regulamentações internacionais para a proteção de dados pessoais, que entram em vigor no dia 25 de maio, impõem uma mudança de postura das empresas brasileiras que ofertam produtos e serviços a partir do monitoramento de comportamentos e de dados pessoais. A GDPR (*General Data Protection Regulation*) foi aprovada e adotada pelo Parlamento Europeu em abril de 2016 e, diferentemente de uma diretiva, sua internacionalização não necessita de legislação aprovada pelos governos. Dessa forma, demandará análises internas sobre como as corporações manuseiam informações de colaboradores, clientes e demais públicos.

A legislação não se aplica somente a organizações localizadas na União Europeia. Sua abrangência se estende a todas que ofereçam produtos e serviços, ou monitorem comportamentos, de dados pessoais de cidadãos europeus e até mesmo outros que estejam apenas de forma transitória na União Europeia. Tais organizações serão obrigadas a criar configurações de privacidade em seus produtos e propriedades digitais. Também precisarão avaliar continuamente os riscos de violação de privacidade, justificar como obtiveram permissão para usar dados e documentar como as informações foram utilizadas.

Entende-se por dado pessoal toda informação que possa servir, direta ou indiretamente, para identificar uma pessoa. Tais dados envolvem nome, foto, e-mail, dados bancários, postagens em redes sociais, informação médica ou endereço IP de um computador. Desse modo, todas as empresas brasileiras que tiverem qualquer relacionamento que envolva o tratamento de dados pessoais com europeus ou até mesmo brasileiros, sejam os que possuem dupla cidadania ou que estejam de passagem pelos países do bloco, estarão sujeitas às novas normas e às penalidades previstas pelo regulamento.

As multas máximas por descumprimento do GPDR, que envolvem casos como não ter o consentimento do usuário para processar seus dados pessoais ou violação de privacidade, chegam a 4% do faturamento bruto anual, podendo atingir 20 milhões de euros. No entanto, existem gradações com relação às penas. Por exemplo, uma companhia pode ser multada em 2% de sua receita bruta anual por não ter os seus registros em ordem (artigo 28 da GDPR), por não notificar a autoridade responsável ou o detentor dos dados pessoais sobre uma falha de segurança ou não conduzir uma avaliação de riscos de sua atividade. É importante notar que essas regras se aplicam tanto aos controladores quanto aos processadores dos dados. Assim, os serviços em nuvem também ficam sujeitos às punições.

Diante da nova lei, as condições para o consentimento do uso de dados pessoais devem ser fortalecidas. Segundo o artigo 29, o consentimento deve ser expresso, ou seja, o titular dos dados precisa responder ativamente a uma solicitação. As companhias não poderão mais fazer longos e ilegíveis termos e condições, prática condenada na GDPR. A requisição desse consentimento deve ser feita pela empresa em linguagem e forma inteligível e fácil, com o objetivo de que o processamento dos dados seja transparente.

Uma das áreas mais afetadas é a de marketing. Com a nova regulamentação, a coleta de dados terá de ser precedida pela explanação de seu propósito. A empresa deve demonstrar como e quem deu o

consentimento e, caso o processamento de dados destine-se a diversos fins, todos deverão ser contemplados. A pessoa tem o direito de retirar a autorização a qualquer momento, e sua saída deve ser tão simples quanto sua concessão.

Já as regulações em torno dos vazamentos de dados estão, primeiramente, relacionadas às regras de notificação das companhias que foram invadidas. Ocorrências que possam colocar em risco indivíduos devem ser relatadas às autoridades e a todos que possam ser afetados, sem atrasos, no prazo de 72 horas.

Para evitar problemas futuros, as empresas devem rever a forma como armazenam e processam dados pessoais, avaliar gargalos e mapear os riscos de descumprimento. Além disso, é preciso designar um responsável para a área, conhecido como Executivo de Proteção de Dados (EPD), que deverá se envolver em praticamente todas as atividades da empresa: desde o desenvolvimento de produtos e serviços até a criação de políticas públicas, aplicando metodologias de *privacy by design* e *data protection by design*. Também será exigida a elaboração de relatórios de impacto à privacidade e proteção de dados pessoais.

Ainda não existe a necessidade legal de um EPD, mas as empresas já devem se organizar nesse sentido, em face dos enormes desafios já fornecidos pelo Código de Defesa do Consumidor e pelo Marco Civil da Internet. Além disso, está em discussão no Brasil o Projeto de Lei 5.276/2016, inspirado na GPDR, que irá regulamentar o tratamento e a proteção de dados pessoais no país. As mudanças provocam um avanço significativo no tratamento de dados, mas requerem a preparação das empresas e a mudança de postura desde já, pois podem até inviabilizar os negócios.

Date Created
23/03/2018