Entrevista: Maurício Tamer, advogado

A Lei Geral de Proteção de Dados é uma mudança de paradigma. Em vez de apenas dizer o que acontece com empresas que cuidarem mal dos dados pessoais sob sua responsabilidade, diz como eles devem ser tratados. Isso envolve todo o modelo de negócio de quem lida com esse tipo de informação. Da coleta ao armazenamento à prestação de serviços.

Por isso, não adianta relegar a política de dados ao jurídico, ou à área de compliance. "Tem que ser uma política total da empresa", afirma o advogado **Maurício Tamer**, da área de *compliance* digital do Opice Blum, Bruno, Brusio e Vainzof Advogados.

Segundo ele, a lei é um exemplo bem sucedido de quando o Direito consegue correr atrás e acompanhar as mudanças da sociedade. Medida mais do que necessária, defende, porque se o Direito ignora a realidade, a sociedade é que passa a ignorar o Direito.

Em entrevista à **ConJur**, o advogado explica que a evolução tecnológica chegou num estágio em que o grande ativo são os dados pessoais dos usuários de serviços e cidadãos. E quem não tomar cuidado pode perder o direito de acesso a esses ativos. "O principal desafio é correr contra o tempo", afirma.

Leia a entrevista:

ConJur — Por que existem tantos vazamentos de dados?
Maurício Tamer — Porque dados pessoais são um grande ativo de mercado. Nos últimos 20 anos, com a internet, com as mídias sociais, com os aplicativos, aconteceu toda essa evolução da tecnologia da informação, o que envolve a captação constante de dados. Dá para fazer uma comparação com a descoberta do petróleo e de suas possibilidades, como aquilo foi importante historicamente e economicamente. Hoje os dados são esse grande ativo. E aí surgiu um quadro dos modelos de negócio baseados nos dados pessoais.

ConJur — A Lei Geral de Proteção de Dados entra em vigor em agosto de 2020. É de fato uma lei

2023 - www.conjur.com.br - Todos os direitos reservados.

importante para o mercado?
Maurício Tamer — É uma lei superimportante. Ela consolida juridicamente a necessidade do uso ético, seguro e legal dos dados dos usuários. Ela mapeia toda a cadeia de utilização dos dados pessoais e diz quais são os fundamentos para o uso correto deles.

A defesa do consumidor é também uma questão importante. A lei diz quais são as obrigações do provedor, do controlador e do operador, as responsabilidades do agente de tratamento de dados, para dizer quem responde pela lei e quais providências devem ser tomadas.

ConJur — Como funciona a responsabilização de empresas estrangeiras?
Maurício Tamer — Se a empresa presta serviços aqui, coleta e trata dados de brasileiros aqui no Brasil, está sujeita às punições da lei. Ou se a empresa usa dados coletados em vários lugares do mundo, mas para prestar serviços aqui, também responde. Isso foi feito porque a lei precisa considerar que não vai ser cumprida também.

ConJur — Como assim?
Maurício Tamer — Para evitar, por exemplo, de alguém deslocar a empresa para fora do Brasil e não se sujeitar à legislação brasileira. A lei amarra: se coletar dados no Brasil ou se usar os dados para prestar serviço no Brasil, está sujeita, tanto às punições quanto à fiscalização. É um paradigma de mudança cultural.

ConJur — Por quê?
Maurício Tamer — Antes o que havia era uma preocupação mais de quem era ligado à área, dos especialistas. A lei vem exatamente para virar essa chave, para demonstrar que a privacidade tem que ser a regra em qualquer modelo de negócio. E o que tenho observado é uma verdadeira corrida de todas as empresas que tratam de dados para se adaptar. Este é o principal desafio: temos que correr contra o tempo.

ConJur — Há algo da lei que ainda cause apreensão?
Maurício Tamer — Uma questão sensível é a que trata das bases de tratamento. Eu posso coletar dados e compartilhá-los se isso estiver dentro do meu "legítimo interesse". A gente vai ter que esperar um pouco a interpretação para ver como vai se acomodar esse legítimo interesse para coletar informações pessoais, e isso só vai vir com a aplicação.

ConJur — Sua área no escritório é "especialista em *compliance* digital". O que é *compliance* digital?
Maurício Tamer — É a adequação ao que diz a lei. A empresa não pode esperar a lei entrar em vigor para se adaptar. A partir de agosto de 2020, ela está sujeita às punições. O compliance digital é buscar essa adequação. O ideal é que seja feito um plano de tratamento de dados, para a empresa estar em conformidade com a legislação e com os novos padrões de tecnologia da informação. E a Lei de Proteção de Dados é clara nesse sentido. Ela diz: "Tem que ter boas práticas de governança de dados e adotar procedimentos internos para assegurar que o tratamento dos dados respeita a lei".

ConJur — E isso é uma nova área dentro da empresa?
Maurício Tamer — O ideal é que se crie um comitê multidisciplinar com vários setores da empresa

2023 - www.conjur.com.br - Todos os direitos reservados.

para instruir profissionais de diversos setores sobre o que eles devem fazer e quais são as consequências de descumprir. Não adianta concentrar só no departamento jurídico ou só na área de *compliance*. Tem que ser uma política total da empresa. O comando tem que dar uma mensagem clara de que aquilo tem de ser feito.

A lei determina que tenha um personagem na empresa responsável pela área de dados. É o que ela chama de "encarregado", que na verdade é uma expressão brasileira do *data protection officer* , que é o DPO [*diretor de proteção de dados, em inglês*]. Além da organização interna, esse executivo vai ser o responsável pela interlocução com as autoridades de fiscalização e com o "relatório de impacto de tratamento de dados pessoais".

ConJur — Que documento é esse?
Maurício Tamer — Uma das exigências da lei. É um relatório de impacto, um mapa de todos os dados tratados, qual a particularidade, se são sensíveis, o que dá pra "anonimizar" e o que não dá, o que pode ser compartilhado. Ou seja: o documento é um mapeamento de todo esse fluxo de informações para que entender o que acontece para, a partir daí, estruturar o cumprimento à lei.

ConJur — O Direito ainda resiste à tecnologia?
Maurício Tamer — Não mais. O Direito é uma ciência social, e tem que se adaptar às mudanças e às necessidades sociais. O problema é que vai ter descompasso entre a evolução do Direito, que passa por questões representativas e de tramitação de projetos, um processo moroso e demorado que passa por bases democráticas de construção de formatação da legalidade em si. Além disso, o Direito é um texto rígido, tem dificuldade de se adaptar a essa realidade que eu chamo de "realidade beta".

ConJur — O que a lei diz sobre esses vazamentos de dados?
Maurício Tamer — A partir da lei qualquer incidente de informações é um ponto de atenção. Nem sempre é o caso de vazamento, muitas vezes a própria empresa ou o órgão público é vítima, há a participação de um hacker, enfim. Do ponto de vista da lei é o seguinte: primeiro, ela notifica que houve um incidente relacionado a dados. Depois, vai ser verificado se esse incidente violou a lei. Pode ser que a empresa tenha adotado todos os parâmetros de segurança e mesmo assim o incidente aconteceu. Aí não houve violação à lei. Se houve, na hora de aplicar sanções, as multas vão até 2% do faturamento até R$ 50 milhões, determinação de publicização da condenação, dar ciência ao mercado, que tipo de dados vazou, se são sensíveis ou não. O tempo de comunicação e a forma de reação também vão definir o parâmetro da sanção a ser aplicada.

ConJur — E em relação ao poder público?
Maurício Tamer — Embora não se fale em *compliance* do poder público, há uma preocupação, que já vem da Lei de Acesso à Informação, para que se divulguem informações de maneira cuidadosa e o governo precisa se organizar nesse sentido. O poder público também é um agente de tratamento de dados e está sujeito à lei. Claro que as sanções são diferentes, mas na ótica da lei, não tem muita diferença.

ConJur — Recentemente, o CNJ suspendeu um contrato entre o TJ de São Paulo e a Microsoft. Um dos argumentos era que o tribunal cedeu seus dados a uma empresa estrangeira, que passaria a ter controle sobre eles. Existe mesmo algum risco nessa contratação?
Maurício Tamer — Quando se fala em dados pessoais, se fala em riscos. Seja o TJ-SP, seja um ente

2023 - www.conjur.com.br - Todos os direitos reservados.

privado, se está tratando de dados pessoais, está assumindo um risco. Por isso a melhor orientação é: só trate aqueles dados pessoais que você precisa para desenvolver suas atividades. Obviamente, o TJ está buscando eficiência, mas precisaria saber especificamente o que a Microsoft vai fazer, se ela vai tratar dos dados, vai ter poder de decisão sobre as informações ou se só o TJ vai decidir. Qualquer tribunal, qualquer órgão público, deve obedecer a lei e deve se preocupar com as contratações, principalmente de empresas privadas.

ConJur — E a Autoridade Nacional de Proteção de Dados. Essa agência vai poder fiscalizar o governo? Porque os membros vão ser escolhidos pelo presidente. Vai ser imparcial?
Maurício Tamer — Existe uma questão em relação à autoridade Nacional muito difícil: ela está na lei, mas tem um vício de origem, a Constituição não permite que lei de iniciativa parlamentar crie órgãos no Executivo. E a Lei de Proteção de Dados criou essa autoridade. Em razão disso, o Poder Executivo vetou, recriando a Autoridade por medida provisória que está em debate no Congresso Nacional. Mas é um órgão absolutamente fundamental, porque centraliza a fiscalização. Ela resolve um problema muito sério que temos no Brasil, de multi-institucionalidade. Na ideia de garantir direitos, criaram-se vários órgãos fiscalizadores, o que traz uma insegurança jurídica muito grande. Então, a ideia da autoridade nacional é ter pessoas especializadas no assunto e também centralizar a fiscalização, para dar segurança jurídica. Com essa agência, as demais perdem o poder de fiscalizar a coleta, uso e armazenamento de dados pessoais.

ConJur — A lei diferencia a coleta de dados para políticas públicas da coleta para fins comerciais?
Maurício Tamer — São coletas completamente distintas. Quando lei diz quais são os fundamentos que autorizam a coleta de dados, estabelece dez bases legais. E distingue a coleta para fins comerciais das políticas públicas. O governo precisa de autorização legal expressa para coleta de dados, por exemplo, mas define qual deve ser o procedimento, as finalidades, diz que o administrador público deve sempre dizer qual é a finalidade da coleta de dados.

Já a coleta para fins comerciais é uma dinâmica completamente diferente. Precisa do consentimento, de legítimo interesse, enfim, para que ela se justifique. Tem que primeiro mapear o cenário, entender as informações que você tem, quais os indivíduos, os dados pessoais.

Date Created
01/05/2019

2023 - www.conjur.com.br - Todos os direitos reservados.