Entrevista: Thiago Sombra, advogado especialista em proteção de dados

O ambiente digital na Europa e, consequentemente, no resto do mundo, passou por uma grande mudança na última sexta-feira (25/5). Entrou em vigor a Regulação Geral de Proteção de Dados (conhecida como GDPR, na sigla em inglês), que é a nova lei europeia de proteção de informações digitais.

As normas valem não só para os membros da União Europeia, mas para todas as empresas e nações que tenham negócios ou algum tipo de relação com a UE que envolva tratamento de dados pessoais. Por "dados pessoais" a GDPR quer dizer dados biométricos, dados de saúde, geolocalização, números identificáveis, dados étnicos, religiosos e opção política.

O advogado **Thiago Sombra** afirma que tanto o governo quanto as empresas brasileiras vão ter de se preparar para a GDPR. E ainda falta muito, diz ele.

Sombra é um grande especialista no assunto. Doutorando em proteção de dados pela UnB, tem pós-graduação na matéria pela London School of Economics e hoje é sócio de Proteção de Dados do Mattos Filho. Recentemente, obteve o certificado europeu de "profissional de proteção de dados", o CIPP/E.

E o diagnóstico que ele faz é que o Brasil não está preparado para manter relações com as empresas europeias. O resultado será fuga de investimentos, diz ele. A principal mudança da GDPR, explica o advogado, é a noção de consentimento para o uso de dados. Agora, as pessoas têm de autorizar ativamente o uso, e não apenas responder "sim" aos pedidos de acesso das empresas.

A GDPR também estipula que um país só atende ao seu padrão de proteção de dados caso tenha uma legislação abrangente que regule o tema e uma autoridade que fiscalize. O Brasil não possui nenhum dos dois requisitos. "O Brasil vai ter um problema comercial grande. Vai começar a chegar contrato da União Europeia para cá dizendo que a gente tem que assinar, dizendo que está cumprindo com os requisitos deles também. Como é que uma empresa brasileira vai dizer que está cumprindo?", alerta Sombra, em entrevista à **ConJur**.

Na Europa, umas das grandes preocupações com a GDPR é o novo patamar de multas que ele impõe para quem descumprir as normas. As penalidades vão de vinte milhões de euros a 4% do faturamento bruto da empresa. A imprensa europeia vem noticiando que 80% das empresas podem quebrar com uma multa desse nível.

Leia a entrevista:

ConJur — Qual é a abrangência da GDPR?
Thiago Sombra — É uma lei de característica extraterritorial e tem como objetivo atingir países que, de alguma forma, têm empresas ou estabelecimentos sediados na União Europeia. Também visa empresas que oferecem bens e serviços na União Europeia, que monitoram comportamentos de usuários sediados na União Europeia e países que, por alguma razão, aplicam o direito europeu por extensão. Guiana Francesa e Suriname, por exemplo.

ConJur — O que a GDPR muda em relação ao que era estabelecido na diretiva de 1998?
Thiago Sombra — O consentimento para o uso dos dados pessoais. O conceito de dado pessoal passa a ser dado biométrico, de saúde, geolocalização, números identificáveis, dados étnicos, religiosos, opção política. Tudo isso passa a ter uma abrangência muito maior dentro do conceito de dado pessoal. Mas o foco da GDPR não é só os dados pessoais, são os dados pessoais transitados de forma automatizada ou automatizável ou que venham a formar um sistema de arquivos.

As sanções agora são mais graves das que já existiam na área diretiva. As multas são de 20 milhões de euros ou 4% do faturamento global da empresa. Outro dia saiu uma reportagem dizendo que hoje, na atual conjuntura, quase 80% das empresas na União Europeia poderiam ir à falência com o valor das multas. Em relação aos dados de criança, será necessário o consentimento dos pais ou do representante legal. Então vai ser mais difícil para redes sociais com foco em crianças, por exemplo.

ConJur — Umas das coisas impostas por essa nova legislação são parâmetros que um país deve atender para poder manter relações comerciais com a União Europeia. Quais são esses parâmetros?
Thiago Sombra — São dois requisitos: ter um marco regulatório completo de proteção de dados e uma autoridade de proteção de dados. O nosso, no Brasil, é um marco regulatório todo fragmentado. As instituições financeiras têm os delas, a gente tem alguns setores regulares. O governo tem o dele. Mas não temos um arranjo completo. Quer dizer, o país tem que ter um arranjo completo, tem que ter todo um arcabouço regulatório de proteção de dados e, simultaneamente, ele tem que ter uma autoridade.

ConJur — O Brasil não atende o padrão de cuidado com os dados que a GDPR impõe. Como vamos então manter relação comercial com o bloco?
Thiago Sombra —

A lei estabelece que, se eu vou transferir dados de um empregado daqui do Brasil para a União Europeia ou de lá para cá, essas transferências de dados entre as empresas multinacionais acontecem por meio de normas corporativas vinculantes. Quando são dados de relações comerciais da minha empresa com outra empresa lá, a gente usa os contratos padrão. Então o Brasil vai ter que se valer dessas duas ferramentas, porque ele não é reconhecido. Só que é caro. São duas ferramentas caras. Você precisa de uma série de mecanismos, tem que ter aprovação das autoridades de proteção de dados dos países para onde você está transferindo dados.

ConJur — Como fica a questão das agências que irão regular o tema?
Thiago Sombra — Cada país deverá ter a sua autoridade de proteção de dados. Será necessário também criar o papel do *data protection officer*. Ele será o responsável por comunicar incidentes. O prazo para a comunicação de um incidente de vazamento é de 72 horas.

ConJur — Alguns são contra criar uma agência reguladora do uso de dados por causa dos custos que isso acarretaria.
Thiago Sombra — Não é cortar gasto, é deixar de ter investimento. Nenhuma empresa europeia vai conseguir transferir dado do Brasil para lá. Simplesmente, o que você vai fazer com isso é afastar investimentos estrangeiros do Brasil. O governo brasileiro vai ser muito pressionado por empresas a tentar aprovar um projeto rápido. Será um embaraço para o nosso relacionamento internacional.

ConJur — Que setor vai ser mais afetado por isso?
Thiago Sombra — Comércio eletrônico. Comércio eletrônico hoje é o que mais movimenta dinheiro no mundo inteiro. Você não vai comprar nada de uma empresa europeia daqui se o Brasil não tiver algum tipo de arranjo que permita essa transferência. O Brasil vai ter um problema comercial grande. Vai começar a chegar contrato da União Europeia para cá dizendo que a gente tem que assinar, dizendo que está cumprindo com os requisitos deles também. Como é que uma empresa brasileira vai dizer que está cumprindo?

ConJur — Quais as diferenças do modelo de regulação da União Europeia e dos Estados Unidos?
Thiago Sombra — A União Europeia tem um modelo de coregulação. Significa que os órgãos reguladores e o Estado traçam normas gerais e a iniciativa privada vai preenchendo os buracos que foram deixados pelo regulador. Nos Estados Unidos existe uma perspectiva mais da autorregulação. Ainda assim há uma regulação geral, existem normas gerais de proteção de dados. Mas o que a gente vê ali é uma atividade maior da iniciativa privada. Então o setor é regulado, você tem uma agência, a FDC, que é responsável pela aplicação dessas medidas. Mas também existe o *private enforcement.*

ConJur — Como funciona isso?
Thiago Sombra — Tenho lá os termos de uso e a política de privacidade do meu site. Estou dizendo para você, usuário, que eu vou te oferecer proteção, dados criptografados, dados anonimizados, vou te permitir colocar os dados em um lugar seguro. Estou te falando tudo isso da minha política. O órgão regulador vai pegar minha política e ver se eu estou fazendo tudo isso que eu disse que ia fazer. Se eu não estiver fazendo, ele vai me punir com base na minha própria política de privacidade. É uma regulação muito moderna.

ConJur — E no Brasil, como funciona?
Thiago Sombra —

O Brasil acha que só por lei vai conseguir disciplinar tudo. Não funciona. A tecnologia é disruptiva e, em virtude da arquitetura da rede, ela é capaz de se rearranjar e alcançar formatos distintos para atingir os mesmos objetivos dela. É o que a gente costuma dizer: não muda o vinho, muda-se a garrafa. Mas o vinho continua o mesmo. A lógica muito utilizada é do código. Então assim: o que você faz para o cara não roubar sua casa? Você coloca uma porta na frente. Se essa porta não for suficiente, você coloca outra porta. Se não for suficiente, você muda o código da fechadura. É assim que funciona o ambiente virtual. Ele não funciona com base na imposição de comportamentos e normas. É ineficiente fazer isso, porque ele vai achar outra forma de atingir aquela finalidade.

ConJur — Correm três projetos de lei no Brasil sobre o tratamento de dados: PL 330, PL 5276 e PL 4060. E um dos debates que têm sido travado nas cortes do Brasil é se as empresas devem manter os dados armazenados no Brasil. O Marco Civil não estabelece isso. Pode uma lei de dados estabelecer?
Thiago Sombra — Territorialidade não é um ponto de discussão no Brasil, nem no Marco Civil nem nesse projeto. Na redação inicial do Marco Civil, a territorialidade era um quesito. Os dados tinham que estar todos no Brasil. Hoje não mais. O Banco Central lançou uma consulta pública recente para que dados fossem hospedados no Brasil. Acabou de sair a resolução e o Banco Central entendeu que não tem como fazer isso mais. No mundo virtual, disruptivo e de convergência, se eu estou tratando com *clouds* [armazenamento de dados em servidores remotos], não tem como limitar isso a fronteiras físicas. É uma contradição de termos. Da mesma forma aqui, com o projeto de proteção de dados. Esses são assuntos de cooperação internacional. Se um determinado dado está hospedado em uma *cloud* que fica na Irlanda, isso é um problema de Direito Internacional Público. Então os dois países têm que se acertar e aprovar um tratado internacional que melhore o processo de cooperação em fornecimento de dados.

ConJur — O GPDR trata de direito ao esquecimento?
Thiago Sombra — O GNPR trata da figura do direito ao esquecimento e prevê a possibilidade de exclusão dos dados do usuário, mas resguarda as empresas a manter cópias quando for para cumprimento de obrigações legais como lavagem de dinheiro, ou para execução de algum contrato futuro ou para a própria proteção da empresa. Então assim: a empresa precisa daqueles dados para eventualmente se proteger em um processo judicial. Então ela prevê essa possibilidade. Mas há também a possibilidade de que o usuário peça a exclusão dos dados quando há o encerramento de uma relação jurídica ou coisa do gênero.

Date Created
27/05/2018