Filipe Fonteles: O impacto da legislação europeia de proteção de dados

Na virada do milênio, a forma de interação das pessoas com computadores e serviços pela internet mudou substancialmente, aumentando o fluxo de dados pessoais que circula na internet[1]. A situação se agravou com o surgimento do *big data*, em que volumes avassaladores de dados são coletados e tratados de maneira constante e em tempo real[2], tornando-se o novo ouro negro[3].

Para lidar com a nova realidade de uso indiscriminado e em larga escala de dados pessoais, a Comunidade Europeia aprovou um novo regramento, denominado General Data Protection Regulation – GDPR, em substituição à Diretiva 95/46/CE, que até o momento regulava a proteção de dados pessoais no âmbito na União Europeia. Sendo uma regulação, o GDPR confere uma proteção mais efetiva do que as diretivas (como a Diretiva 95/46/CE), por ter força cogente e não depender de leis nacionais dos Estados-membros para sua eficácia[4].

O GDPR entrará em vigor na próxima sexta-feira (25/5) e prevê novas obrigações aplicadas a sociedades empresárias que coletam ou processam dados pessoais, estejam ou não em território europeu, com vistas a aumentar o controle e a responsabilização por eventuais danos aos cidadãos daquela comunidade[5]. O alcance internacional das regras de proteção aos dados pessoais foi um dos principais nortes que guiaram a elaboração do GDPR[6].

Para sociedades brasileiras que ofereçam produtos ou serviços ao público da União Europeia, ou que simplesmente coletem dados de pessoas em um ou mais dos seus Estados-membros, com ou sem fins lucrativos, as regras do GDPR devem ser observadas e aplicadas, sob pena de sofrerem medidas corretivas ou até sanções pecuniárias.

Toda e qualquer captação de dados pessoais feita em território europeu de forma regular (ou seja, não pontual) está sujeita às regras do GDPR[7]. Isso se aplica tanto à coleta e ao tratamento de dados de usuários para fins de publicidade dirigida quanto à realização de um simples cadastramento de cliente para concretizar uma venda em site de *e-commerce*.

Objetivamente, empresários brasileiros devem prestar atenção nas regras do GDPR por dois motivos: a partir do dia 25, fica proibida a transferência de dados entre sociedades europeias e sociedades estrangeiras (inclusive brasileiras), salvo se atendidas condições do GDPR; além disso, empresários que coletem dados pessoais em território europeu ficam obrigados a constituir um representante em um dos Estados-membros da UE.

Como o Brasil ainda não foi reconhecido pelas autoridades europeias como um país que detém legislação de proteção de dados pessoais adequada[8][9], o fluxo de dados para nosso território dependerá de garantias adequadas a serem fornecidas pelo controlador ou processador das informações (GDPR, artigo 46, 1)[10].

As *garantias adequadas* podem ser de oito tipos[11]. Na prática, salvo se for negociado algum acordo especial entre entidades governamentais brasileiras e europeias, o que ainda não se tem notícia, a opção que se apresenta como menos burocrática para empresários brasileiros é a adoção das chamadas *regras vinculativas aplicáveis a sociedades*

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

(*binding corporate rules*).

Por envolver somente um contrato entre sociedades (que contenha tais *regras vinculativas*), trata-se de uma solução menos burocrática e de rápida implementação. Porém, tal permissivo legal do GDPR só se aplica à transferência de dados entre sociedades de um mesmo grupo econômico, sendo que uma das sociedades precisa estar localizada em território europeu, o que limita a abrangência da norma.

No caso de transferência de dados entre sociedades que não pertençam ao mesmo grupo econômico, outras opções devem ser buscadas, como cláusulas contratuais entre o controlador ou processador de dados em território europeu e o controlador ou processador de dados no Brasil, seguindo os moldes aprovados pelas autoridades europeias, o que inclui a designação de um representante legal na União Europeia para responder às autoridades locais em nome da sociedade brasileira (artigo 27).

Nesse caso, o representante deverá estar fisicamente localizado em um dos Estados-membros da União Europeia e terá o papel de interagir com a autoridade de controle, se necessário.

Sociedades que violarem o GDPR poderão receber medidas corretivas como advertências ou ordem de suspensão temporária do tratamento de dados. Nos casos mais graves, penalidades de multa poderão ser aplicadas, esteja o infrator dentro ou fora do território europeu.

A pena será graduada conforme as circunstâncias do caso, incluindo a natureza, a gravidade e a duração da infração, o âmbito ou o objetivo do tratamento de dados, o número de titulares afetados, o caráter intencional ou negligente da infração e o grau de cooperação com a autoridade de controle a fim de sanar a infração, dentre outros critérios (GDPR, artigo 83, 2). A multa pode chegar a 20 milhões de euros ou, no caso de uma sociedade empresária, até 4% do seu volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, o que for maior (GDPR, artigo 83, 5, “c”).

Se por um lado a nova regulação europeia confere um nível de proteção às pessoas naturais elevado e sem precedentes, por outro lado haverá um grande impacto — e custo — para que os prestadores de serviços se adaptem às suas regras.

No universo de sociedades empresárias de grande porte, tais custos serão facilmente absorvidos por suas estruturas já complexas. Todavia, no caso de empresas de pequeno porte ou mesmo *startups*, o custo para a remodelagem do negócio e, principalmente, para a constituição ou indicação de um representante local será significativo.

Como uma empresa que deseja prosperar na economia atual não pode abrir mão do uso de *big data*, soluções criativas certamente serão criadas, sejam jurídicas ou de arquitetura do negócio.

Para a realidade brasileira, espera-se que o Congresso Nacional se sensibilize e aprove uma lei geral de proteção de dados nacional. Há alguns projetos de lei sobre o tema atualmente em tramitação, alguns muito alinhados com as regras do GDPR[12], o que poderá levar nosso país a ingressar na seleta lista de países reconhecidos pelas autoridades europeias como possuidores de regras adequadas, o que, automaticamente, afasta as rígidas exigências para a transferência internacional de dados.

Em suma, diante dos reflexos que o GDPR pode produzir sobre negócios já estabelecidos entre

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

empresários brasileiros e europeus, com implicações em contratos, políticas internas e até estrutura de negócios, trata-se de um tema que deve estar na ordem do dia.

[1] CATE, Fred H.; CULLEN, Peter; MAYER-SCHÖNBERGER, Viktor. CATE, Fred H.; CULLEN, Peter; MAYER-SCHÖNBERGER, Viktor. *Data Protection Principles for the 21st Century:* revising the 1980 OECD Guidelines (2014), p. 6.
[2] MCKINSEY&COMPANY. *Big Data, Analytics, and the Future of Marketing & Sales* (eBook). New York: McKinsey&Company, 2013.
[3] Wu, Tim. *Impérios da Comunicação:* do telefone à Internet, da AT&T ao Google. Tim Wu; tradução Claudio Carina – Rio de Janeiro: Zahar, 2012, p. 384.
[4] IT GOVERNANCE PRIVACY TEAM, EU *General Data Protection Regulation (GDPR):* an implementation and compliance guide. IT Governance Publishing, Ely, Cambridgeshire (UK), second edition, 2017.p. 2.
[5] MANTELERO, Alessandro e VACIAGO, Giuseppe. *Legal aspects of information science, data science, and Big Data*. In Frontiers in Data Science. Dehmer, Matthias; Emmert-Strein, Frank (Coord.). CRC Press, 2018.
[6] HUSTINX, Peter. *The Reform of EU Data Protection:* towards more effective and more consistent data protection across the EU. Versão revisada da palestra proferida na Universidade de Fribourg, em 15/6/2012, durante o 5º Dia da Lei de Proteção de Dados da Suíça. Disponível em (https://edps.europa.eu/sites/edp/files/publication/13-01-15_speech-fribourg_en.pdf), acessado em 10/3/2018, p. 8.
[7] O Art. 49 do GDPR prevê a derrogação de suas regras para transferência de dados desde que a transferência não seja regular e que atenda aos seguintes requisitos:
a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;
b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva;
d) A transferência for necessária por importantes razões de interesse público;
e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;
f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;
g) A transferência for realizada a partir de um registo que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto.
[8] O Brasil ainda não possui uma lei geral de proteção de dados pessoais, embora o Marco Civil de

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

2014 já tenha representado um significativo avanço nessa seara.
[9] A lista publicada sob a égide da Diretiva 95/46/CE contempla 12 nações, incluindo dois países latino-americanos (Argentina e Uruguai).
[10] GDPR. Artigo 46. Transferências sujeitas a garantias adequadas.
1. Não tendo sido tomada qualquer decisão nos termos do artigo 45, no. 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.
[11] O Art. 46, itens 2 e 3 do GDPR prevê os seguintes tipos de garantia adequada:
a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos brasileiros e europeus;
b) Regras vinculativas aplicáveis às sociedades empresárias nos termos do artigo 47 do GDPR;
c) Cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia;
d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controle e aprovadas pela Comissão Europeia;
e) Um código de conduta acompanhado de compromissos vinculativos e com força executiva assumidos pelo controlador ou processador de dados;
f) Um procedimento de certificação acompanhado de compromissos vinculativos e com força executiva assumidos pelo controlador ou processador dos dados;
g) Cláusulas contratuais entre o controlador ou processador de dados em território europeu e o controlador ou processador de dados no Brasil; ou
h) Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.
[12] Vale destaque para o PL 5.276/2016.

Date Created
19/05/2018

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