Opinião: O que podemos aprender com a Europa após 1 ano da GDPR

O marco regulatório europeu sobre privacidade e proteção de dados pessoais, a *General Data Protection Regulation* (GDPR), fez o seu primeiro aniversário de eficácia plena neste mês de maio. O regulamento, que substituiu a Diretiva 95/46/CE, estabelece novos princípios, padrões e regras para o tratamento de dados pessoais, a fim de endereçar de maneira assertiva e atualizada o desenvolvimento tecnológico pós-década de 1990, principalmente com o surgimento de redes sociais, da utilização comercial de *Big Data* em diversos setores da economia e do marketing comportamental.

Neste cenário, a coleta significativa de dados pessoais se tornou realidade, e a monetização desses ativos para os mais diversos fins econômicos refletiu em uma necessária regulamentação, como forma de assegurar direitos e liberdades fundamentais por meio da privacidade e proteção aos dados pessoais de pessoas naturais. Fato é que a regulamentação traz uma significativa motivação para a alteração de *mindset* durante a realização de negócios na atual economia movida a dados, além de ter gerado um grau maior de conscientização por parte dos titulares de dados pessoais.

Para entender os efeitos práticos da GDPR na sociedade após um ano, vejamos abaixo alguns números interessantes.

GDPR em números
De acordo com o trabalho realizado pela *European Commision*[1] e a *International Association of Privacy Professionals* (Iapp), no período de quase 12 meses após sua entrada em vigor:

- 67% dos europeus ouviram em algum momento a respeito da GDPR;
- 57% dos europeus sabem que existe uma autoridade pública responsável pela proteção de dados pessoais;
- foram realizadas aproximadamente 144.376 reclamações às autoridades de proteção de dados europeias por supostas violações à GDPR;
- 89.271 notificações de *data breach*[2] foram apresentadas para as autoridades europeias de proteção de dados;
- 500 mil entidades localizadas na chamada *European Economic Area* (EEA) registraram *Data Protection Officers* (DPOs) perante as autoridades europeias[3];
- a aplicação da GDPR resultou em um montante de multas no valor de aproximadamente 56 milhões de euros.

Resultados das principais autoridades europeias[4]
A autoridade austríaca de proteção de dados foi a primeira a aplicar uma multa relacionada a descumprimento da GDPR, enquanto a CNIL, autoridade francesa, registrou 310 investigações em 2018 relacionadas ao novo regulamento europeu de proteção de dados. Na maioria dos casos, o resultado foi o aprimoramento do *compliance* nas entidades investigadas. Os setores mais afetados pela fiscalização foram as *seguradoras e empresas especializadas em marketing direcionado por meio de aplicativos*.

Por sua vez, a ICO, autoridade britânica, informou ter recebido cerca de 39.825 notificações entre maio de 2018 e abril deste ano a respeito de possíveis violações à GDPR. Os três principais assuntos levantados pelos titulares de dados pessoais foram: acesso a dados pessoais, divulgação de dados pessoais e a restrição ao processamento de dados. A entidade teve uma grande atuação na conscientização a respeito da GDPR pela publicação de diversos *guidelines* a respeito do tema.

Ainda, quase que instantaneamente após a entrada em vigor do regulamento, a *Data Protection Comission*, autoridade referência na Europa, iniciou investigações com foco na vigilância pelo poder público de titulares de dados pessoais, tais como pela utilização de *drones*, câmeras e outras tecnologias.

Quanto aos efeitos da GDPR no Brasil, além de a regulamentação europeia ter servido como fato motivador e influenciador da nossa Lei Geral de Proteção de Dados (LGPD), sua aplicação extraterritorial da GDPR, bem como as regras para transferências internacionais de dados pessoais, são alguns dos principais pontos de preocupação para empresas brasileiras.

Em um cenário de momentânea instabilidade em relação à criação de uma Autoridade Nacional de Proteção de Dados Pessoais, diante do impasse na conversão da MP 869/18 em lei, que deverá ocorrer até o dia 3 de junho, o Brasil enfrenta o risco de não ser reconhecido como um país adequado para o fluxo de dados de cidadãos europeus, o que torna mais burocrática, complexa e arriscada a recepção de dados provenientes do território europeu. Essa posição coloca o Brasil atrás de países da América do Sul, como Argentina e Uruguai, que já são considerados como adequados e desimpedidos para receber dados protegidos pela regulamentação europeia, o que, obviamente, facilita negócios na economia digital movida a dados.

De toda forma, a principal lição que podemos extrair da GDPR (repetida pela LGPD) se baseia na necessidade de se instituir uma nova cultura para as organizações, partindo da premissa de que o titular está no controle de seus dados. Com isso, as organizações com presença nacional podem se valer das lições aprendidas durante os 12 meses de aplicação da GDPR como *benchmarking* para adequar suas operações e garantir a conformidade com a lei brasileira, mitigando riscos, danos financeiros e reputacionais, possibilitando, ainda, um relevante potencial competitivo para seus clientes e demais *stakeholders*. Ou seja, é hora de aprendermos com os erros e acertos da Europa com relação à adequação à GDPR, a fim de nos prepararmos bem para a versão tupiniquim do regulamento: a tão falada LGPD.

[1] Disponível em: https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf. Acessado em: 23/5/2019.
[2] Segundo a GDPR, a empresa que tiver conhecimento de um vazamento de dados deve notificar a autoridade competente em até 72 horas.
[3] Disponível em: https://iapp.org/media/pdf/resource_center/GDPR_at_One_IAPPWhitePaper.pdf . Acessado em: 23/5/2019.
[4] Disponível em: https://iapp.org/media/pdf/resource_center/GDPR_at_One_IAPPWhitePaper.pdf . Acessado em: 23/5/2019.

Date Created
31/05/2019