View this email in your browser

Editorial
TelComp

Lei Geral de Proteção de Dados chegou. E agora?

Por Rafael Pistono, Raphael Campos e Cecília Cunha
Vinhas e Redenschi Advogados

É com prazer que trazemos para os nossos leitores um artigo sobre a Lei de Proteção de Dados, que entra em fase final de tramitação e que trará impactos importantes sobre tratamento de dados pessoais no Brasil.

Já é lugar comum afirmar-se que nesse século os dados têm o valor que tinha o petróleo no passado.

Com certeza, as possibilidades de uso criativo de dados coletados através dos milhões de interações na internet, crescem e tendem ao infinito!

Mas isto impõe às empresas novas obrigações e mudanças importantes sobre tratar dados pessoais daqui para frente.

Como contribuição para a análise do tema, trazemos hoje artigo da equipe do Escritório **Vinhas e Redenschi Advogados**, cujo sócio **Rafael Pistono** é membro do Conselho de Administração de nossa associada **Angola Cables** e também do Conselho Consultivo da

Ontem, dia 10 de Julho de 2018, foi aprovada a **Lei Geral de Proteção de Dados** pelo Senado Federal. Essa nova legislação, que, após sanção Presidencial, entra em vigor depois de 18 meses da sua publicação oficial, promete ser o início da incorporação de uma cultura real de privacidade e proteção de dados no Brasil, alterando a forma como as organizações coletam, gerenciam e protegem dados pessoais.

Resultado de um importante movimento mundial, a iniciativa busca inserir o Brasil no rol de países considerados maduros[1] pela Comunidade Europeia na tutela dos dados pessoais e no âmbito adequado de utilização desses bens, já que, em uma nova lógica econômica, qualquer atividade quer aproveitar ao máximo o poder de obter e reter dados, como um caminho efetivo para ganhos de competitividade e produtividade.

TelComp.

As informações e opiniões contidas no artigo são de inteira responsabilidade dos autores e não necessariamente refletem os posicionamentos da TelComp.

Boa leitura!

Em um cenário regulatório fragmentado com normas esparsas e setoriais, a Lei Geral aprovada reflete os impactos do *General Data Protection Regulation - GDPR,* sentidos principalmente através da busca pela adaptação de empresas brasileiras ao "padrão global de

proteção de dados" estabelecido pelo regulamento, tendo em vista o seu amplo âmbito de aplicação. O GDPR entrou em vigor na Comunidade Europeia no dia 25 de maio de 2018*,* revogando a Diretiva 95/46 e reforçando a necessidade de se respeitar o direito do cidadão à proteção de seus dados, afetando qualquer organização que "trate" dados de pessoas localizadas na UE, independentemente de a organização estar ou não estabelecida na Comunidade ou da nacionalidade do titular dos dados. A aplicação do Regulamento se dá, por exemplo, para empresas brasileiras que simplesmente ofertem serviços / produtos no diploma recém aprovado, é o de "*privacy by design*", importantíssimo em um mundo altamente digitalizado, movido por dados e no qual as *startups* estão ganhando cada vez mais espaço. Esse conceito busca equacionar a proteção de dados pessoais desde a criação do produto ou do serviço, de forma preventiva e proativa, através de uma configuração padrão de privacidade e proteção que objetiva atingir funcionalidade completa e segurança de ponta a ponta. É quando a ideia de privacidade nasce com a própria empresa.

Objeto de grandes expectativas, a

(onerosamente ou não) ao mercado europeu, assim como à empresa que, mesmo sem presença física na União Europeia, terceirize o processamento de dados para as empresas localizadas na União Europeia. Em suma, esse regulamento é aplicável a qualquer tipo de relação comercial com titular de dados estabelecido na União Europeia, seja ele cidadão europeu ou não.

O novo diploma protetivo, guardadas as devidas peculiaridades e características, tem bastante semelhança com a regulamentação europeia, uma vez que dela extrai importantes conceitos e princípios, respectivamente em seus artigos 5º e 6º. Dentre as diversas similaridades trazidas pelo Projeto de Lei Geral de Proteção de Dados Brasileira do GDPR, está o caráter extraterritorial da LGPD, visto que independentemente do país da entidade, a legislação brasileira ganhará e alcançará as organizações que realizem atividades de (i) tratamento de dados no Brasil, (ii) tratamento com objetivo de ofertar ou fornecer bens e serviços em território brasileiro, ou (iii) tratamento de dados coletados em território brasileiro.

Ao titular e detentor do dado pessoal deverão ser assegurados os direitos de (i) livre acesso aos dados pessoais, (ii) confirmação da existência de tratamento, (iii) correção de dados incompletos ou inexatos, (iv) anonimização, bloqueio

LGPD pretende viabilizar a criação de uma Autoridade Nacional de Proteção de Dados Pessoais, autarquia especial vinculada ao Ministério da Justiça que tem, dentre outras atribuições, a função de avaliar o nível de proteção de dados de outros países quando houver transferência internacional, tendo também o dever de zelar pela proteção dos dados pessoais e realizar ou determinar a realização de auditorias no âmbito da atividade de fiscalização. Tal autoridade deverá ter como característica a independência administrativa e ausência de uma subordinação hierárquica.

Portanto, superando muitas dúvidas e desconfianças acerca de sua aprovação em 2018, a Lei Geral de Proteção de Dados promete trazer segurança e esclarecimentos ao relevante tema da privacidade e proteção de dados pessoais, permitindo que as organizações, privadas e públicas, possam desenvolver suas atividades em um ambiente transparente e alinhado com as melhores práticas.
O primeiro passo é entender que dado pessoal, nos moldes do GDPR, deve ser considerado qualquer informação relativa a uma pessoa física identificada ou identificável, de maneira que podem ser considerados dados pessoais o nome, número de identidade/CPF, dados de localização, biometria, dados de saúde, dados genéticos, opiniões políticas, orientação sexual, IP etc.

ou eliminação de dados que são desnecessários, a portabilidade, apagamento, informação sobre o compartilhamento de dados e revogação do consentimento.

Será preciso ter especial atenção à coleta indiscriminada de dados, sendo o consentimento o requisito básico para que os dados pessoais sejam tratados. Esse consentimento deverá ser apresentado de forma bem expressa e destacada, sempre em linguagem clara e simples, e sua retirada deverá ser tão fácil como a sua concessão. Por outro lado, existem outras formas de tratar os dados pessoais, sem o consentimento (quando, por exemplo, for necessária a obtenção do dado para a execução de um contrato, para o cumprimento de uma obrigação legal, para a defesa de interesses vitais do titular, para o exercício de funções de interesse público ou para a persecução de interesses legítimos).

Importante conceito que surge com o regulamento europeu, e é refletido

Sem perder de vista a efetividade do novo diploma, é certo que o legislador trouxe pesadas sanções que poderão chegar a 2% do faturamento (com limitação de R$ 50 milhões de reais). As multas serão aplicadas de acordo com a infração, devendo-se levar em consideração faltas e transgressões anteriores, gravidade, categoria, dolo, medidas de segurança adotadas, cooperação com as autoridades etc.

É exatamente pelo fato de que nem sempre o vazamento pode ser evitado que, mais do que nunca, é tão importante e necessário estar *compliant,* demonstrando que as medidas para antever e minimizar os riscos foram tomadas, e GDPR ou LGPD são, em verdade, oportunidades para as organizações criarem, por meio de programas próprios e específicos, uma cultura de respeito à privacidade e proteção de dados pessoais.

---

[1] A Comissão Europeia reconheceu Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jersey, Nova Zelândia, Suíça, Uruguai e os EUA (limitado ao quadro do Privacy Shield) como proteção. Estão em andamento conversas com o Japão e a Coréia do Sul que podem vir a embasar uma decisão de adequação.

Nosso endereço de e-mail é:
editorial@telcomp.org.br

Você recebe este e-mail por ter relacionamento com a TelComp.