Proteção de dados no Brasil e no mundo

Uma leitura do que vigora hoje, a importância da nova legislação e como as empresas e os entes públicos devem se preparar

Dustin Pozzetti, Sócio-líder de Regulação e Telecom;
Emerson Melo, Sócio-líder de Compliance;
Leandro Augusto Marco Antonio, Sócio-líder de Cyber Security;
Marcelo Ribeiro, Sócio-diretor de Regulação e Telecom;
Marcos Matsunaga, Sócio da Ferraz de Camargo e Matsunaga Advogados;
Marina Bozzola, Gerente da Ferraz de Camargo e Matsunaga Advogados.

O avanço das tecnologias de coleta, processamento e interpretação de dados pessoais traz oportunidades infinitas para conhecer os hábitos e padrões comportamentais de usuários de serviços e de plataformas tecnológicas disponibilizadas pelas organizações (ex. *sites, apps*, entre outros), permitindo gerar ações de marketing mais eficientes e customizadas em setores de consumo, serviços, setor financeiro e de seguros, entre outros, e até mesmo no plano das recomendações de políticas públicas. Na era digital, os dados converteram-se em patrimônio das empresas que os detêm, gerando a necessidade de conferir-lhe algum grau de proteção jurídica e regulação que garantam transparência e apliquem os preceitos constitucionais do direito à vida privada.

A recém aprovada Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), visa a assegurar que princípios de respeito e proteção de dados não serão negligenciados, e apesar de entrar em vigor no Brasil apenas em fevereiro de 2020, tem gerado inúmeras interrogações nos agentes de mercado. Globalmente, o tema proteção de dados vem sendo tratado há mais de 40 anos (tabela 1) e sofre atualizações recorrentes na medida em que o processo de inovação supera o desenho inicial do arcabouço, como por exemplo na União Europeia. Ela utilizou cerca de 90% das bases da Diretiva 95/45 para criar a General Data Protection Regulation (GDPR) que inclui, entre outros, seções sobre consentimento explícito, notificação sobre vazamentos, direito ao acesso, direito à exclusão dos dados, DPO (*Data Protection Officer*), RoP (*Required Organizational Pratices*), portabilidade dos dados, privacidade desde a concepção, previsões de multas, além de uma linguagem direta e simples.

No total, mais de 100 países têm leis específicas voltadas à proteção de dados dos cidadãos e alguns dispõem de uma Autoridade Supervisora de Dados independente, com poderes para garantir a obediência à codificação. Em todos os países nos quais houve aderência à lei, percebeu-se melhoria na dinâmica dos negócios, bem como uma maior necessidade de repensar estratégias e, especialmente, de se analisar a maneira como estas serão executadas pelo negócio. O prazo

Tabela 1 - Visão geral do tema Proteção de Dados Pessoais em outros países

OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	União Europeia: Diretiva nº 95/45/EC, substituída pela Regulamentação Geral de Proteção de Dados (GDPR)	Reino Unido: Ato de Proteção de Dados	Japão: Ato de Proteção de Informações Pessoais	Alemanha: Ato Federal de Proteção de Dados (Bundesdatenschutzgesetz)
Em vigor desde 1980	Em vigor desde 1995	Em vigor desde 1998	Em vigor desde 2005	Em vigor desde 1998
Estados-membros devem ter legislação interna focada na proteção da privacidade e dos direitos individuais. Exigências de privacidade atingem entes públicos e empresas privadas.	Uniformiza diretrizes para proteção de dados pessoais em todos os Estados-membros. Determina que direitos individuais devem ser protegidos e assegurados. Previne abusos.	Impõe regras relativas à proteção a dados pessoais e aos "dados sensíveis", que englobam informações como religião professada e etnia.	Empresas e demais organizações públicas ou privadas devem salvaguardar direitos e interesses dos indivíduos no processamento de seus dados. Prevê sanções penais em caso de desrespeito às disposições do Ato.	Protege os interesses individuais no que tange ao uso de dados pessoais. Uma curiosidade interessante: a primeira lei de proteção alemã a dados individuais data de 1977 e já estendia aos entes públicos e privados a responsabilidade pelo bom uso desses dados e respeito à privacidade.

de 18 meses no Brasil, contados da data de sanção da LGPD, em 14 de agosto de 2018, para que as empresas possam adaptar-se à nova realidade e cumprir a lei em sua totalidade é enxuto para regularizar o banco de dados existente e começar a tratar os novos dados coletados.

De acordo com a Pesquisa KPMG International: *Guardians of trust – Who is responsible for trusted analytics in the digital age*, datada de fevereiro de 2018, 92% dos executivos não confiam no processo de Data Analytics da sua empresa, o que torna altamente recomendável a contratação de um prestador externo de serviços. A KPMG conta com um conjunto de capacidades e experiência assessorando clientes nacionais e internacionais para estabelecer a total aderência da operação com a estratégia de negócio e recomenda atenção especial para os seguintes pontos:

1 – Estabelecer princípios que permitam ao usuário conhecer e gerenciar os dados que são obtidos pela entidade: além do consentimento explícito, caberá à empresa que recebe essas informações municiar o usuário com tudo o que ele precisa saber acerca das políticas de privacidade dos sites que frequenta, tendo o direito de visualizar, corrigir e excluir dados que tenham sido coletados. O tratamento das informações será permitido se estiver dentro das hipóteses previstas na proposta, como obrigações legais, contratuais e proteção do crédito.

2 – Adotar um conjunto de controles que permitam manter a guarda somente dos dados dos usuários ativos e habilitar um processo seguro de portabilidade: dados pessoais deverão ser excluídos após o encerramento da relação entre o cliente e a empresa; os titulares das informações poderão corrigir dados que estejam de posse de uma empresa; a transferência de dados pessoais só poderá ser feita a países com nível "adequado" de proteção de dados

3 – Manter trilhas de auditoria para os princípios de causalidade: uma das passagens mais interessantes da lei determina que, para cada decisão automatizada feita por uma empresa, ela deve ser capaz de explicar como chegou a ela.

4 – Implantar e aprimorar sistemas de segurança da informação: além de as empresas coletarem somente os dados necessários aos serviços prestados, deverão existir medidas de segurança para proteger os dados pessoais de acessos não autorizados e de "situações acidentais ou ilícitas" de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Criptografar esses dados e assegurar o direito do usuário ao anonimato estão previstos, com o objetivo de coibir a exposição dos usuários em eventuais vazamentos. Cabe ao responsável pela gestão dos dados o dever de comunicar casos de "incidente de segurança" que possam trazer risco ou dano ao titular das informações – por meio, por exemplo, de vazamentos ou ataques de *hackers*.

5 – Mecanismos para suportar possível "responsabilidade solidária": a lei estabelece papéis e responsabilidades entre controladores e operadores em caso de violações, com possível aumento de ações civis pelos titulares de dados em caso de vazamentos. Assim, a expectativa é de que as organizações se debrucem com mais cuidado sobre as decisões de uso de dados e informações, além de melhor definição da relação e dos controles entre empresas, bem como mais rigidez e segurança no manejo de dados dos usuários por parte do Poder Público.

6 - Implementar um programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado à estrutura geral de governança, e estabeleça e aplique mecanismos de supervisão internos e

externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. Cumpre lembrar que, de acordo com a legislação, é preciso "demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei", e que: "§ 3º – As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional".

Adequar-se aos novos tempos será a melhor maneira de as empresas atuantes no Brasil não serem atingidas pelas multas previstas (veja box). Anunciantes e marcas que lidam com diferentes provedores, ou até com bases proprietárias de dados, precisarão estar mais atentos aos processos de coleta e armazenamento de informações que venham a adquirir e utilizar, dada a questão, já mencionada, de responsabilização solidária. É possível que muitas empresas precisem ampliar investimentos em ferramentas tecnológicas e na contratação de profissionais altamente capacitados para as áreas de tecnologia da informação, assessoria jurídica e segurança cibernética. Elas também terão de revisar contratos com prestadores de serviço, fornecedores, colaboradores etc. Ou seja: terão de investir tempo, dinheiro e energia na adequação regulatória.

Cabe ressaltar que a nova lei tem uma vantagem: ela não cria regras pontuais que poderiam, no futuro, tornar-se inadequadas ou ultrapassadas. Ao contrário: seus princípios e fundamentos, alinhados ao que existe de mais moderno no mundo contemporâneo, elevam o tratamento de dados no Brasil a patamares aptos a fazer frente aos maiores avanços tecnológicos. ■

Multas

No que se refere às multas, a nova legislação estabelece que:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração.