Valéria Reani: Impactos da LGPD nos negócios e nas pessoas

Primeiramente, vale ressaltar que o Brasil possui mais 30 diplomas legais sobre o assunto — aí se inclui a própria Constituição Federal, o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e o Código Civil.

A Constituição Federal, em seu artigo 1º, III, preceitua que um dos fundamentos do Estado brasileiro é a dignidade da pessoa humana. Para alguns doutrinadores, esse princípio é a guia para a tutela efetiva de todos os direitos fundamentais contidos na Carta Magna de 1988. Mais a frente, no mesmo diploma legal, em seu artigo 5º, X, preceitua que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", ficando evidente a proteção dos direitos da personalidade, que também ficam claros no artigo 21 do Código Civil, ao preceituar que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma", protegendo a intimidade e a vida privada, possuindo grande ligação com a questão da proteção dos dados pessoais sob a ótica europeia, consubstanciada no artigo 8, nº 1 da Carta dos Direitos Fundamentais da União Europeia.

Por sua vez, a Lei 8.078/90 (Código de Defesa do Consumidor), em seu artigo 43, trata da questão do acesso por parte do consumidor aos dados pessoais que estejam arquivados — "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes" —, mostrando uma preocupação do legislador com essa questão, sendo que o referido artigo do CDC possui forte ligação com o artigo 5º, LXXII, ao prever o remédio constitucional conhecido como habeas data, ao preceituar que: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Mais recentemente ocorreu a entrada em vigor da Lei 12.965/14, o Marco Civil da Internet, que poderia ter resolvido, de certa forma, esse vácuo legislativo existente no Brasil, já que o arcabouço jurídico pátrio não possui norma efetiva que tutele a proteção de dados pessoais e seu tratamento, porém se limitou a tratar de forma tímida em seu artigo 11 a questão da proteção dos dados pessoais, deixando, ainda, um campo aberto para regulação. Depois foi a vez da Lei 12.527/2011 (Lei de Acesso à Informação – LAI), decorrente do artigo 5º, XXXIII, artigo 37, parágrafo 3º, II e o artigo 216, parágrafo 2º, todos da CF/88, com o direito constitucional da privacidade. O primeiro possibilita o recebimento de informações públicas dos órgãos estatais e propicia maior liberdade de opinião e de expressão, enquanto o segundo protege e assegura os direitos à privacidade e à intimidade que provêm da própria natureza humana e daí o seu caráter inviolável, intemporal e universal, impedindo a devassa nas informações de cunho estritamente pessoal.

Então, qual o objetivo da Lei Geral de Proteção de Dados? A lei objetiva garantir ao cidadão:

- direito à privacidade: garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras,

visando garantir direitos e liberdades fundamentais;
- regras claras para empresas: estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para empresas;
- promover desenvolvimento: fomentar o desenvolvimento econômico e tecnológico numa sociedade movida a dados;
- direito do consumidor: garantir a livre-iniciativa, a livre concorrência e a defesa do consumidor;
- fortalecer confiança: aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais;
- segurança jurídica: aumentar a segurança jurídica como um todo no uso e tratamento de dados pessoais.

Quanto à importância da Lei Geral de Proteção de Dados, podemos destacar:

- unificar regras: regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia;
- adequar as regras no Brasil: tornar o Brasil apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação;
- portabilidade: indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade no mercado.

A LGPD tem aplicação tanto no âmbito público e privado quanto on-line e offline. Ela versa sobre o conceito de dados pessoais:

- lista as bases legais que autorizam o seu uso, com o consentimento do titular dos dados pessoais, permitindo o uso de dados com base nos legítimos interesse do controlador;
- trata de princípios gerais, direitos básicos do titular — como acesso, exclusão dos dados e explicação sobre uso —, obrigações e limites que devem ser aplicados a toda entidade que se vale do uso de dados pessoais, seja como insumo do seu modelo de negócio, seja para a atividade de seus colaboradores.

Eis os 10 princípios/razões que devem ser levados em consideração no tratamento de dados pessoais:

- finalidade: propósito legítimo para uso dos dados pessoais;
- adequação: compatibilidade de tratamento com a finalidade;
- necessidade: uso e tratamento dos dados ser restrito ao mínimo necessário;
- livre acesso: garantia de consulta facilitada e gratuita sobre a integralidade de dados, forma e duração do tratamento;
- qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados de acordo com a finalidade de seu tratamento;
- transparência: garantia de informação precisa sobre o tratamento dados;
- segurança: utilização de medidas técnicas capazes de garantir a segurança do tratamento;
- prevenção: adoção de medidas para prevenir a ocorrência de danos, em função do tratamento inadequado;
- não discriminação: impossibilidade de tratamento para fins discriminatórios, ilícitos e abusivos;
- da responsabilização e prestação de contas, que obriga o responsável pelo tratamento dos dados

pessoais a demonstrar de forma cabal e transparente a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados.

Quanto aos principais pontos da Lei Geral de Proteção de Dados, temos:

- aplicação transversal, multissetorial, a todos os setores da economia, tanto no âmbito público quanto privado, on-line e offline;
- aplicação extraterritorial: em moldes similares à regulamentação europeia, a *General Data Protection Regulation* (GDPR), a lei geral, ou seja, o dever de conformidade superará os limites geográficos do país. Toda empresa estrangeira que, com filial no Brasil, ou oferecer serviços ao mercado nacional e coletar e tratar dados de pessoais naturais localizadas no país estará sujeita à nova lei;
- traz conceito amplo do que deve ser considerado dado pessoal informação relacionada à pessoa natural/física, identificada ou identificável. Ou seja, qualquer dado que isoladamente ou agregado a outro possa permitir a identificação de uma pessoa natural, ou sujeitá-la a um determinado comportamento;
- define dados pessoais sensíveis como aqueles que, pela sua própria natureza, podem sujeitar o seu titular a práticas discriminatórias, tais como dados sobre a origem racial ou étnica, a convicção religiosa, a opinião política, dado referente à saúde ou à vida sexual; ou permitir a sua identificação de forma inequívoca e persistente, tais como dado genético ou biométrico;
- conceitua dados anonimizados que seriam os relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dados efetivamente anonimizados são essenciais para o funcionamento de tecnologias e da Internet das Coisas, inteligência artificial, *machine learning*, *smart cities*;
- fala também de dados públicos, tais como os constantes de bases geridas por órgãos públicos, publicações oficiais e cartórios, ou os expressamente tornados públicos pelos seus titulares, como em perfis públicos em redes, ficando o uso desses dados limitado às finalidades.

Proteção dos dados pessoais de crianças
Objetivando manter a integridade dos pequenos, como nome, endereço e escolaridade, entre outros, que só poderão ser usados pelas empresas após consentimento dos responsáveis dos menores de 12. Maiores de 12 anos poderão consentir, desde que entendam do que se trata aquele termo. Por isso, eles devem ter linguagem clara e acessível.

Os direitos básicos dos titulares de dados
Dentre os direitos listados, destaca-se o de acesso aos dados, retificação, cancelamento ou exclusão, oposição ao tratamento, de informação e explicação sobre o uso dos dados.

O direito à portabilidade dos dados, que, similar ao que pode ser feito entre diferentes empresas de telefonia e bancos, permite ao titular não só requisitar uma cópia da integralidade dos seus dados que facilite a transferência destes para outros serviços, mesmo para concorrentes.

Responsabilidade dos agentes de tratamento: os diferentes agentes envolvidos no tratamento de dados — o controlador e o operador — podem ser solidariamente responsabilizados por incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou pela não conformidade com a lei.

Ressalte-se que a LGPD, determina a a nomeação de um Data Protection Officer (DPO), cuja tradução e "encarregado", responsável pelo tratamento de dados pessoais dentro da organização.

Qual o impacto nos negócios e atividades?
A LGDP não afeta somente os grandes *players* do setor de tecnologia e serviços on-line, como aqueles oferecidos pelo Google e Facebook, mas também qualquer organização que realize uma operação de coleta, uso, processamento e armazenamento de dados pessoais, no âmbito de atividades de bancos, corretoras, seguradoras, clinicas médicas, hospitais, e-commerce, varejo, hotéis, companhias aéreas, agências de viagens, restaurantes, academias, entre muitas outras, podem estar sujeitas à aplicação da lei, ainda que tais atividades ocorram exclusivamente fora do ambiente digital.

Quem está sujeito a LGPD? Quais regras devem ser observadas pelas empresas do setor publico e privado?

- a definição e documentação da base legal que autoriza o tratamento de dados (que podem incluir, mas não se limitam, a definir se o tratamento é realizado com base no consentimento, para fins de cumprimento de obrigação legal, para a execução de contrato, ou com base no interesses legítimo);
- o atendimento aos direitos concedidos aos titulares de dados, como o direito de obter informações sobre o tratamento de dados, realizar o acesso, retificação e eliminação de dados, direito à portabilidade a outro fornecer de produtos e serviços e obter a revisão de decisões automatizadas, dentre outros;
- a nomeação de um *encarregado* ou *Data Protection Officer* (DPO), responsável pelo tratamento de dados pessoais dentro da organização;
- a notificação a autoridade competente, em caso de incidente (divulgação e/ou uso não autorizado de dados pessoais);
- a adoção de medidas de (organizacionais e técnicas para) proteção de dados, a partir da criação de qualquer nova tecnologia ou produto (*privacy by design*); e
- adequação às hipótese que autorizam a transferência de dados para fora do país, quando aplicável.

Quais informações são consideradas como dados pessoais?
Dados pessoais podem compreender qualquer informação relacionada a uma pessoa natural, identificada ou identificável. Neste sentido, dados de pessoas jurídicas não são cobertos pela LGPD, mas somente informações relacionadas às pessoas físicas. Um segundo aspecto importante é relacionado ao fato de que dados pessoais podem consistir em qualquer informação de pessoas identificadas ou identificáveis. Dados pessoais de indivíduos identificados são aquelas informações que imediatamente podem identificar uma pessoa, como o nome, número de CPF e RG e informações de documentos pessoais.

A LGPD regula o tratamento de dados pessoais em relações de clientes e fornecedores de produtos e serviços, prestadores e tomadores de serviços, empregados e empregadores, e demais relações nas quais dados pessoais sejam recebidos, enviados e/ou processados.

As atividades de processamento de dados dentro e fora do país estão sujeitas a lei?
Operações de tratamento de dados realizadas dentro do território brasileiro estão sujeitas a aplicação da LGDP. Além de operações de tratamento realizadas dentro do país, quando o tratamento tiver por objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos

localizados no território brasileiro, a lei também pode se aplicar, ainda que a organização responsável por essa atividade esteja sediada ou localizada fora do país. Assim, o local onde os dados são tratados não é requisito único ou preponderante para aplicação da lei, sendo também importante identificar a localização do indivíduo cujos dados serão coletados.

Quem não está sujeito à lei?
O uso pessoal para fins particulares e não econômicos, para fins jornalísticos, artísticos ou acadêmicos, não estão dentro do escopo da lei e, portanto, aos requisitos de tratamento de dados. Da mesma forma, o tratamento de dados para fins de segurança pública, defesa nacional, segurança do estado e/ou atividades de investigação e repressão de infrações penais também não estão sujeitos a LGPD, e estão sujeitos a regulação de legislação específica no tema. Dados provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento podem eventualmente não estar sujeitos a aplicação da lei.

Qual o risco do não cumprimento da lei?
As penalidades por descumprimento da LGPD incluem advertência, obrigação de divulgação do incidente, eliminação de dados pessoais, bloqueio, suspensão e/ou proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais, multa, chegando ao valor limite de R$ 50 milhões por infração.

Por fim, desde o último dia 14 de agosto o Brasil passou a ter não somente uma importante legislação específica que regulamenta o tratamento de dados pessoais, tanto pelo poder público quanto pela iniciativa privada que traz as novas regras criadas como meio de fortalecer a proteção da privacidade dos usuários , como também um grande desafio técnico, jurídico e cultural. O *vacatio legis* é de 18 meses de sua publicação oficial, isto quer dizer que o interregno para a estruturação empresarial privado e publico acontece nos próximos 18 meses, quando entrará em vigor a lei , mais precisamente, em fevereiro de 2020.

Conclusão
Assim, o Brasil conta com uma robusta legislação em termos de proteção de dados pessoais, o que possivelmente aprimorará o desenvolvimento tecnológico, práticas de negócios, crescimento do mercado digital e ao mesmo tempo proteção aos dados pessoais dos cidadãos em nosso país.

Outrossim, um cuidado que se deve ter é com a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela supervisão, fiscalização e a disseminação de boas práticas entre as empresas públicas e privadas, sob pena de ausência de confiança do mercado, priorize um engajamento construtivo com a indústria, no seguinte sentido de que ao invés de inquisição e sanção, dar prioridade ao diálogo, apoio, mutua cooperação, orientação, conscientização e informação; além de estimular relações abertas e construtivas com negócios que lidem com dados pessoais, primando pela boa-fé das empresas e nos seus esforços em cumprir a lei; bem como propiciar a criação de ambientes para inovações responsáveis, como *Regulatory Sandboxes*, nos quais novos projetos podem ser testados em atmosferas controladas visando avaliar eventuais e futuras necessidades regulatórias, conforme o caso, mas *a posteriori*.

As sanções devem ser a *ultima ratio*, principalmente e somente quando houver alguma violação dolosa, ou práticas exponencialmente negligentes, condutas reiteradas ou extremamente graves.

Ter um órgão controlador de todo esse processo é ideal e essencial para que ele seja sempre gerenciado conforme a lei. No entanto, enquanto uma nova agência é criada pelo Executivo e enquanto as empresas estão em período de preparação e adaptação às novas mudanças, é possível ir tomando medidas de auditorias dentro das próprias empresas sobre seus dados atuais, além da possibilidade da contratação de um *encarregado* — já que, assim, o oficial de dados atribui a responsabilidade de processadores e controladores de informações à uma pessoa. O desafio das empresas para estar em conformidade com a lei é importante e pode se tornar uma vantagem competitiva mais pra frente.

Referência bibliográfica
LEI 13.709, DE 14 DE AGOSTO DE 2018 – Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Date Created
25/10/2018