Ariana Quintanilha: LGPD como pilar do compliance

17/05/2022

A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em agosto de 2020, é o marco regulatório da proteção de dados e que estabelece regras para o processamento, armazenamento e gerenciamento de dados de pessoas naturais.

Essa lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Este marco seguiu os moldes da GDPR (*General Data Protection Regulation*), Lei da União Europeia, e entrou em vigor cinco meses do início da pandemia da Covid-19, que obrigou o mundo e, neste caso especificamente os brasileiros, a usarem mais a internet sem qualquer salvaguarda.

O acesso à internet já era um crescente no Brasil, tanto é que segundo o Instituto Brasileiro de Geografia e Estatística (IBGE) em 2017 eram 70,5% dos domicílios que estavam conectados à rede e em 92,7% das residências, pelo menos um morador possuía telefone celular. E com o crescimento desse acesso à internet, via telefone celular, o que em 2016 correspondia a 60,3% dos domicílios, em 2017 passou para 69%, já que as pessoas passaram a utilizar a rede também para compras, pagamento e utilização de redes sociais.

Com a pandemia da Covid-2019, os números — que já eram uma crescente — aumentaram ainda mais e, segundo a Associação Brasileira de Comércio Eletrônico (ABComm), em parceria com a Neotrust, o crescimento nas vendas foi de 68% no período pandêmico, elevando a participação do e-commerce no faturamento total do varejo, que passou de 5% no final de 2019 para um patamar acima de 10% em 2020.

Esses números mostram que as pessoas passaram a usar mais a internet para todo o tipo de serviço, tornando o consumo virtual sem controle, sem organização e sem segurança, o que

acarretou um maior número de dados pessoais e sensíveis circulando pela internet, deixando o consumidor cada vez mais exposto.

Segundo o autor Bruno Bione, qualquer dado pessoal é dotado de importância e valor. Essa noção é percebida no artigo 5º, que fornece as definições de conceitos da LGPD. Sendo dado pessoal toda informação relacionada à pessoa natural [pessoa física] identificada ou identificável; e dados pessoais sensíveis, o dado pessoal sobre origem racial/étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Para Danilo Doneda, essa distinção entre os dados é feita sobretudo a partir do aumento de riscos potenciais apresentado entre um grupo e outro.

Dessa forma, a pandemia acelerou esse processo de utilização desenfreada da internet, e apesar de ser uma facilitadora, requer muita atenção e cautela, tanto do consumidor quanto das organizações. Prova disso foram os inúmeros vazamentos ocorridos somente no período de pandemia, que reforçaram inúmeras fragilidades quanto à segurança de dados no Brasil e a necessidade de uma norma específica sobre o tema, reforçando ainda mais a necessidade de estar em conformidade com a LGPD.

Numa pesquisa feita pela empresa norte-americana Akamai, especializada em tecnologia, o Brasil ocupa a terceira posição no ranking mundial de roubo de dados pessoais na internet. Segundo o relatório anual de segurança cibernética da Trend Micro 2020, somente no ano de 2020 foram detectadas 119 mil ameaças cibernéticas por minuto à medida que o trabalho em home office cresceu e a infraestrutura ficou mais vulnerável e sob pressão de ataques.

Tais exemplos reforçam a necessidade de as empresas buscarem alternativas que tragam segurança aos titulares de dados e que, em contrapartida, também permita que as empresas minimizem os riscos e impactos com esse tipo de incidente de segurança, já que não estar em conformidade com a LGPD pode acarretar sanções administrativas de até R$ 50 milhões ou 2% do faturamento anual da empresa; até a descontinuidade do uso de dados por um período de seis meses ou de forma definitiva. No entanto, as empresas devem olhar para a LGPD pelo que realmente é — uma grande oportunidade de negócios.

Essas experiências têm tornado o mercado mais exigente, seja do ponto de vista do consumidor, seja do ponto de vista das próprias empresas. Até porque a preocupação com essa conformidade deve estar presente cada vez mais nas contratações, eis que o operador (que recebe os dados e realiza o tratamento de dados em nome do controlador) responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador (compete as decisões referente ao tratamento de dados pessoais, artigo 42).

A verdade é que o mercado busca empresas que possuam processos cada vez mais transparentes, e como dito por Hanna Thó, ética não se torna apenas um princípio, mas, agora, uma obrigação das empresas para que a economia se mova. E a LGPD é parte dessa nova era, e foi criada com o intuito de proteger os dados e minimizar os danos com os vazamentos, que são

inúmeros.

Dessa forma, a LGPD se torna um pilar do compliance justamente porque o compliance é uma forma de controle e cumprimento das leis e normas que todas as empresas estão sujeitas.

O termo compliance tem origem na língua inglesa, na expressão "*to comply*", que em livre tradução significa estar em conformidade. Estar em compliance representa estar em conformidade com as normas e regulamentos vigentes, minimizando riscos e mantendo a organização dentro da legalidade.

No Brasil o *compliance* veio à tona a partir da Lei 12.846/2013, conhecida como "Lei Anticorrupção", que prevê, dentre outras questões, a responsabilização das organizações pela prática de atos lesivos à administração pública.

Assim, diante da preocupação das empresas quanto à possibilidade de arcar com sanções severas no âmbito de um processo administrativo de responsabilização, o *compliance* se torna um instrumento de controle de processos e sustentabilidade empresarial.

Franciso Mendes e Vinícius Carvalho descrevem:

"*Um programa de* compliance *visa estabelecer mecanismos e procedimentos que tornem o cumprimento da legislação parte da cultura corporativa. Ele não pretende, no entanto, eliminar completamente a chance de ocorrência de um ilícito, mas sim minimizar as possibilidades de que ele ocorra, e criar ferramentas para que a empresa rapidamente identifique sua ocorrência e lide da forma mais adequada possível com o problema.*"

A relação entre o compliance e a LGPD é permeada pela noção de controle e transparência, visto que a LGPD permite que o titular de dados tenha total controle de todo ciclo de vida dos seus dados dentro de uma empresa, permitindo entender o objetivo e finalidade daquele determinado tratamento. Portanto, na sociedade e no mercado atuais, o controle e transparência são peças-chaves.

A exigência da conformidade é uma forma de manter o mercado competitivo, ao passo que a LGPD pode ser o primeiro caminho para obter uma visão clara do negócio, assumindo o controle dos dados armazenados e gerenciados pela empresa.

Os dados são os principais ativos de uma empresa atualmente, pois pelo viés da LGPD o tratamento de dados é qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Portanto, estar em conformidade com a LGPD é obter maior controle e transparência dos dados dentro de uma empresa, do início ao fim, entendendo as deficiências e aplicando as melhores práticas, aumentando os controles e melhorando o desempenho de toda a empresa.

Em abril deste ano, por exemplo, o McDonald's admitiu um novo vazamento de dados ocorrido por meio de um dos prestadores de serviço e que acabou permitindo o acesso não autorizado a dados pessoais de alguns dos clientes. Segundo a Lei, dados pessoais são informações relacionadas à pessoa natural identificada ou identificável, como por exemplo nome, estado civil, endereço, e-mail, CPF e número de telefone.

O incidente de segurança foi informado à ANPD, que está apurando, mas muito além de multas, quando ocorre um vazamento de dados, as consequências são inúmeras, a começar pela insegurança que isso causa aos clientes e investidores, além da perda de credibilidade e valor da empresa no mercado.

A própria Lei incentiva a criação de boas práticas e estrutura de governança no artigo 50, quando estabelece que as organizações poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e requerimento dos titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Estamos diante de um cenário que atrela uma norma recente sobre a proteção de dados, que nunca foi valorizada no Brasil, a muitas pessoas consumindo cada vez mais a internet. Essa nova prática requer um esforço de todos, uma mudança de cultura reconhecendo a importância de valorizar e cuidar dos dados de uma pessoa.

A solução para essa virada de chave não virá rápido, mas é preciso começar. E um processo de *compliance* robusto, devidamente empregado na prática, que traga controle e transparência do ciclo de vida dos dados dentro de uma empresa, será capaz de transmitir mais segurança e garantir uma boa reputação para a empresa, o que, por fim, gera novas oportunidades de negócios demonstrando compromisso com a lei e a ética.

Referências

https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor
MENDES, Francisco Schertel; CARVALHO, Vinícius Marques de. Compliance: concorrência e combate à corrupção. São Paulo: Trevisan Editora, 2017, p. 31.
https://g1.globo.com/economia/noticia/2021/02/26/com-pandemia-comercio-eletronico-tem-salto-em-2020-e-dobra-participacao-no-varejo-brasileiro.ghtml
https://www.convergenciadigital.com.br/Gestao/Se-vazar-dados%2C-quase-metade-das-empresas-nao-sabe-o-que-fazer-com-a-LGPD-58581.html
https://www.avellareduarte.com.br/internet-no-brasil-2020estatisticas
BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 59.
https://capitalist.com.br/cerca-de-109-milhoes-de-cpfs-cnpjs-e-placas-de-veiculos-sao-expostos-em-site/
DOMINGUES, Paulo de Tarso. Governança, compliance e corrupção. São Paulo: Almedina, 2019.
DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei

geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.
MARCHETTI, Anne M. Beyond Sarbanes-Oxley Compliance: *Effective enterprise risk management.* Hoboken: John Wiley & Sons, 2005.
THÓ, Hanna. Compliance nas empresas estatais brasileiras. Evolução e perspectivas trazidas pela Lei nº 13303 de 2016. Jus Navigandi, nov., 2016. Disponível em: < https://jus.com.br/artigos/54136/compliance-nas-empresas-estatais-brasileiras>. Acesso em: 04 de maio de 2022

Fonte: https://conjur.jumps.com.br/2022-mai-17/ariana-quintanilha-lgpd-pilar-compliance/