REGEN
Revista de Gestão, Economia e Negócios
v. 4, n. 2 (2025) | ISSN: 2676-0185

Enterprise Risk Management (ERM), Segurança Digital e Conformidade Legal: Uma Análise da Lei Geral de Proteção de Dados pela Ótica da Gestão de Riscos Corporativos

Gabriel Barroso Fortes[a,†]
[a]Universidade de Fortaleza (Unifor), Brazil • [†]Autor correspondente: gabriel.b.fortes@gmail.com

INFORMAÇÕES DO ARTIGO

Palavras-chave:

Lei geral de proteção de dados
Enterprise Risk Management
Segurança digital
Gestão de riscos
Governança em privacidade

RESUMO

A presente pesquisa teve por intuito analisar os impactos da Lei Geral de Proteção de Dados no mercado brasileiro, do ponto de vista da gestão dos riscos que as organizações passam a enfrentar pela imposição de novas obrigações sobre a coleta, a utilização ou o compartilhamento de informações ligadas às pessoas. A pesquisa revelou que o crescente movimento de digitalização da economia não só está transformando o modo como as organizações administram suas informações de negócio em meios digitais e passam a atuar no ambiente online, mas também acaba ensejando a regulação do mercado de modo a proteger a privacidade e a individualidade das pessoas, diante dos riscos advindos da utilização de dados pessoais sem limites ou condições transparentes. Nesse sentido, foi observado que, embora existam recomendações técnicas e políticas para que as empresas gerenciem os riscos digitais em nível estratégico, a maioria das organizações brasileiras não parece priorizar os cuidados com segurança da informação, sequer adotando políticas internas para minimizar os riscos envolvidos. Os resultados mostraram, porém, que a LGPD traz uma série de exigências para as organizações, gerando inúmeras situações de risco, tanto de conformidade quanto de segurança. Mas a própria lei prevê um instrumento adequado para auxiliar na estruturação da Enterprise Risk Management (ERM), que pode permitir integrar a gestão dos riscos de conformidade e de segurança da informação à estratégia da organização. Concluiu-se, porém, que, enquanto não for priorizada a adequada gestão dos riscos ligados à LGPD, as organizações brasileiras estão expostas, cada vez mais, a impactos negativos que podem tomar dimensões significativas e até interromper os negócios.

1. Introdução

Em 14 de agosto de 2018, foi publicada no Brasil a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), que consolidou regras e estabeleceu uma nova regulação sobre o modo como as organizações podem e devem tratar informações ligadas aos indivíduos.

A publicação da lei está ligada à percepção de que a digitalização da economia acontece conforme cresce a conectividade entre as pessoas e as organizações passam a estruturar seus negócios a partir de estratégias orientadas por dados, principalmente dados pessoais.

Partindo do pressuposto de que a utilização de suas informações pessoais pode gerar benefícios, mas também danos para o indivíduo, a LGPD tem como objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (art. 1º), sendo as suas normas aplicáveis ao tratamento de dados realizado por qualquer organização:

> Art. 3º. Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I — a operação de tratamento seja realizada no território nacional;
>
> II — a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
>
> III — os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Nesse contexto, é importante destacar que o termo "tratamento" é definido pela própria lei como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X).

Ou seja, a definição de "tratamento de dados" é, como se pode ver, um conceito aberto, pois abrangeria basicamente todo tipo de ação realizada com informações relativas a pessoas, não sendo viável delimitar quais tipos de atividade envolvendo dados pessoais estariam ou não enquadrados na previsão legal.[1]

Além disso, a LGPD define como dado pessoal qualquer "informação relacionada a pessoa natural identificada ou identificável", ou seja, praticamente todo tipo de dado que permita, através da sua leitura técnica, individualizar alguém, ainda que de maneira indireta ou mediante combinação de informações complementares.

Conjugando-se essas premissas, parece adequado inferir que provavelmente todas as organizações lidam com informações de indivíduos (sejam consumidores, empregados, sócios, contratados, acionistas, fornecedores, parceiros, representantes etc.), e, por conseguinte, realizam alguma forma de tratamento de dados pessoais, ou seja, praticamente todas as organizações estão sujeitas à LGPD — fato que denuncia, por sua vez, a relevância do estudo da lei para o mercado.

Até porque a própria LGPD impõe sanções administrativas para a organização que cometer alguma infração às suas regras, as quais vão desde uma advertência formal, com indicação de prazo para adoção de medidas corretivas, até a proibição total do exercício de atividades relacionadas a tratamento de dados, passando pela aplicação de multas, dentre outras penalidades (art. 52).

Demais disso, as organizações que, durante o tratamento de dados, ou em razão de realizá-lo, causarem algum dano a alguém, violando a legislação, estarão obrigadas a repará-lo (art. 42).

Portanto, como se pode antever, o impacto da nova regulação tende a ser muito sensível no mercado, pois, estando praticamente todas as organizações submetidas à LGPD, ficam sujeitas às sanções administrativas e à responsabilidade por danos, se descumprirem a legislação.

Por outro lado, os casos de ameaças e de incidentes de segurança informacional aumentam a cada ano, levando a consequências econômicas e sociais significativas para organizações públicas e privadas, o que tem aumentado os custos financeiros do mercado, principalmente por causa de vazamento de dados.[2]

Portanto, à medida que o governo cria regulamentos para garantir às pessoas a proteção de suas informações individuais, as organizações precisam assumir, cada vez mais, o protagonismo e a iniciativa de liderar a adoção de padrões de privacidade e de gerenciamento de dados que possam acompanhar as novas demandas e necessidades.[3]

Até porque isso se torna uma expectativa crescente no mercado, uma vez que a proteção à privacidade tende a ser uma característica do futuro, isto é, dos serviços, produtos e sistemas a serem disponibilizados no mercado, pois as próprias organizações passam a investir em tecnologias que protejam dados pessoais, o que será cada vez mais necessário à medida que a automação e a Inteligência Artificial (IA) tornam-se mais comuns nos espaços públicos e privados.[4]

Nesse contexto de nova regulação, responsabilidades legais e expectativas de privacidade, parece ser adequado que as organizações adotem, cada vez mais, métodos e práticas de gerenciamento de riscos, de modo a lidar de maneira preventiva com as consequências negativas relacionadas à LGPD.

De fato, além das sanções legais, incidentes de segurança digital podem afetar as organizações em várias dimensões valorativas, causando danos à imagem, prejuízos financeiros, ineficiência operacional, interrupção do negócio etc. Por consequência, a falta de segurança pode diminuir a competitividade, atrasar a capacidade de inovação e afetar a posição da organização no mercado.

Como as atividades econômicas sempre envolvem riscos de todo tipo, também essas variáveis precisam ser gerenciadas, para que as organizações consigam minimizar a frequência e o impacto negativo desses incidentes e, de maneira segura, explorar as vantagens e possibilidades da transformação digital.

O intuito do presente estudo, então, é analisar a relação e a relevância da gestão de riscos para as organizações sujeitas à regulação prevista na lei geral de proteção de dados, o que será realizado através de pesquisa bibliográfica e qualitativa, lastreada em livros, notícias, legislação, relatos de pesquisa etc.

2. Segurança da Informação e Riscos Digitais

O aumento significativo da coleta, do processamento e do compartilhamento de dados pessoais, estimulado pelo desenvolvimento tecnológico e pela globalização digital promovida pela internet, tem criado desafios à proteção da privacidade e exigido, por consequência, um quadro regulatório compatível com a ordem jurídica vigente (Albani, 2019, p. 30).

Nos últimos anos, governo e mercado enfrentam os desafios da transformação digital no Brasil, de modo a aproveitar seu potencial para o desenvolvimento social e econômico, mas também sendo necessário lidar com a proteção à privacidade individual.

[1] Nesse sentido é importante também mencionar o art. 4º da LGPD, que ressalva explicitamente a sua aplicação em determinadas situações: "Art. 4º. Esta Lei não se aplica ao tratamento de dados pessoais: I — realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II — realizado para fins exclusivamente: (a) jornalístico e artísticos; ou (b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III — realizado para fins exclusivos de: (a) segurança pública; (b) defesa nacional; (c) segurança do Estado; ou (d) atividades de investigação e repressão de infrações penais; ou IV — provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei".

[2] Disponível em: https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

[3] Disponível em: https://www.sciencefocus.com/future-technology/new-technology-trends-2020s/

[4] Disponível em: https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF-2/Accenture-Technology-Vision-2020-Full-Report.pdf

Mas essa preocupação não é restrita à realidade brasileira, porquanto revela uma característica da economia global, na verdade:

> "É que, no mundo atual, amplamente permeado pelo uso de tecnologias que dependem de dados, impera o vigilantismo como modelo de negócios, o que, de um lado, é excelente para o preciso direcionamento de produtos e serviços e, por outro, é péssimo para a privacidade das pessoas" (Crespo e Camargo, 2018, p. 180–181).

Assim, conforme avança a digitalização dos negócios em escala mundial, cresce também a preocupação com a segurança da informação, tanto para proteger a privacidade das pessoas, quanto para prevenir perdas nas organizações.

Essa tem sido, por exemplo, uma das pautas recorrentes da Organização para Cooperação e Desenvolvimento Econômico (OCDE), entidade internacional criada para estimular o crescimento econômico e o comércio mundial, e que, no escopo da transformação do mercado, tem monitorado as práticas de gerenciamento de riscos de segurança digital nas organizações.

Em atenção aos desafios da economia digital, a OCDE publicou um documento oficial chamado de "Recomendações do Conselho sobre Gestão de Riscos de Segurança Digital para Prosperidade Econômica e Social", com o intuito de estabelecer diretrizes para boas práticas no mercado.[5]

As recomendações da OCDE estão traduzidas em dois pontos iniciais, que se mostram fundamentais para a boa gestão de riscos na economia digital.

Em primeiro lugar, deve-se partir do pressuposto de que os riscos de segurança digital não podem ser vistos como uma questão simplesmente técnica, como se fossem preocupação de algum departamento ou setor, mas devem ser apreendidos, isto sim, como uma questão econômica, que integra toda a estrutura de gestão de risco das organizações e dos processos de tomada de decisão (OCDE, 2015, p. 4).

Ademais, é somente através do gerenciamento dinâmico que os riscos de segurança digital podem ser reduzidos até um nível que possa ser considerado aceitável em relação aos benefícios econômicos esperados das atividades. Ou seja, as medidas de segurança digital devem ser concebidas de forma a terem em conta os interesses das pessoas envolvidas, serem adequadas e proporcionais ao risco enfrentado, sem prejudicar a própria atividade econômica a proteger (OCDE, 2015, p. 4).

Em suma, justamente porque os riscos ligados à segurança da informação devem ser levados em conta no plano estratégico da organização, toda a estrutura institucional deve estar preparada para gerenciá-los continuamente, de modo que eles não virem obstáculo para viabilizar o cumprimento da estratégia definida.

A apreensão desses conceitos parece ser oportuna para a gestão adequada dos riscos ligados à Lei Geral de Proteção de Dados, pois a segurança digital não pode se limitar aos interesses gerenciais da organização, devendo levar também em conta a perspectiva da legislação (OCDE, 2015, p. 19).

Ademais, embora a LGPD regulamente o uso de informações pessoais em qualquer tipo de suporte, inclusive em meios físicos,[6] é indiscutível que praticamente todas as operações de dados realizadas com conotação de negócio acontecem através de aplicações digitais — daí a pertinência da abordagem pela perspectiva do risco digital.

Ainda nesse contexto, OCDE (2015, p. 8) expressa o risco de segurança digital — o que é mais conhecido no Brasil como risco de segurança da informação — como uma categoria de risco corporativo, relacionado à utilização, desenvolvimento e gestão do ambiente digital no decurso de qualquer atividade econômica.[7]

Por conseguinte, o gerenciamento desse tipo de risco deve se traduzir num conjunto de ações coordenadas dentro da organização para lidar com a segurança digital, buscando maximizar as oportunidades do uso das tecnologias (OCDE, 2015, p. 8).

A gestão da segurança digital, assim, deve ser uma abordagem flexível e ágil, mas integrada à estrutura geral de governança da organização, de modo a permitir lidar com incertezas e alcançar os benefícios esperados, além de proteger os indivíduos contra ameaças, principalmente à questões de privacidade.

Todavia, pode-se dizer que a realidade brasileira é significativamente distante daquilo que recomendam as boas práticas de segurança e privacidade, sendo a publicação da LGPD — muito recente na história legislativa brasileira — uma mostra da necessidade de incentivar a mudança desse quadro.

E os números parecem confirmar essa leitura coloquial.

De acordo com o relatório "TIC Domicílios — 2018", publicado pelo Comitê Gestor da Internet no Brasil (CGI.br), através do Núcleo de Informação e Coordenação do Ponto BR (NIC.Br), por exemplo, 59% dos usuários de internet domiciliar já deixaram de fazer compras online por questões relacionadas à segurança e privacidade.[8]

Já o relatório "TIC Empresas — 2019" — que tem como foco o uso das Tecnologias de Informação e Comunicação (TIC) no mercado brasileiro, e serve para mapear tanto o grau de digitalização dos negócios, quanto o nível de

[5] Embora o Brasil não seja um membro formal da OCDE, o próprio organismo tem monitorado os indicadores do mercado brasileiro, o que mostra a pertinência das suas recomendações para o desenvolvimento socioeconômico do País.

[6] Conforme diz o texto legal: "Art. 1º. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

[7] É importante conferir também a publicação da OCDE "Measuring digital security risk management practices in business". Disponível em: https://www.oecd-ilibrary.org/science-and-technology/measuring-digital-security-risk-management-practices-in-businesses_7b93c1f1-en

[8] Disponível em: https://cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf

comprometimento com a segurança digital — também revela a discrepância, conforme análise de Cantoni et al. (2020, p. 144):

> "[...] os dados retratam que poucas empresas implementam ações para informar os funcionários sobre os riscos digitais, tais como treinamentos (21%) ou discussão sobre esse tema em suas reuniões (33%); além disso, é reduzido o percentual de empresas que indicaram, por exemplo, ter contratos de trabalho que mencionem segurança digital (22%) ou incentivos de desempenho para redução de risco de digital (18%)".

A título de exemplo, conforme o relatório "TIC Empresas — 2019", pode-se verificar que, do total de 7.019 organizações averiguadas na pesquisa, apenas 41% possuíam uma política de segurança digital (ou política de segurança da informação).

Cumpre salientar que tal pesquisa abrangeu todas as regiões do País, em variadas áreas de atuação, sendo possível identificar, inclusive, que somente no setor de "informação e comunicação" a existência de uma política de segurança digital faz parte da realidade da maioria das organizações (65%), o que provavelmente está ligado à compreensão que as pessoas envolvidas nessa área têm sobre a sensibilidade dos ativos digitais.

Já nos demais segmentos pesquisados — indústria de transformação; construção; comércio, reparação de veículos automotores e motocicletas; transporte, armazenagem e correio; alojamento e alimentação; atividades imobiliárias, atividades profissionais, científicas e técnicas, atividades administrativas e serviços complementares; artes, cultura, esporte e recreação, outras atividades de serviços — a proporção de organizações que adotam alguma política de segurança da informação é minoritária.[9]

Ou seja, a breve análise desses dados revela como a preocupação com os aspectos gerenciais da segurança digital — como estabelecer normas formais de segurança — ainda não refletiria a realidade da maioria das organizações do mercado brasileiro.

Destaque-se, ademais, que todas as organizações que foram levantadas na pesquisa têm acesso livre à internet, ou seja, são organizações conectadas à rede mundial de computadores, estando portanto expostas a todas as interações possíveis que são proporcionadas no meio digital.[10]

Mas uma ressalva é necessária, pois a pesquisa foi realizada entre abril e agosto de 2019, portanto, antes de entrar em vigor a LGPD,[11] fato que, por um lado, demonstra o provável despreparo das organizações para atender as normas da lei, mas revela, por outro, a oportunidade que as obrigações legais podem ensejar para que a segurança digital seja priorizada no mercado.

E essa expectativa pode ter sido contemplada, pois, no relatório seguinte, a pesquisa "TIC Empresas — 2021" revelou o aumento do número de organizações que, pelo menos, já possuem uma política de segurança da informação, que subiu para 50% (cinquenta por cento). Ademais, outros setores da economia — transporte, armazenagem e correio (52%); e atividades imobiliárias, atividades profissionais, científicas e técnicas, atividades administrativas e serviços complementares (68%) — também passaram a ser majoritários na adoção desse tipo de norma corporativa.

Mesmo assim, o resultado dessas pesquisas ainda demonstra a disparidade entre o cenário brasileiro e as recomendações da OCDE, segundo as quais o gerenciamento da segurança digital deveria ser visto como componente da própria gestão da organização, ou seja, uma questão estratégica.

Nesse contexto, torna-se oportuna a aproximação das organizações brasileiras com o conceito de *Enterprise Risk Management*, o que é conhecido pela sigla ERM, e que pode ser traduzido como "gestão de riscos corporativos".

O intuito da ERM é desenvolver um conjunto de políticas, procedimentos e controles visando à implantação de mecanismos de gerenciamento de risco do negócio, o que envolve vários aspectos e recortes de cada organização (Nakamura, sd, p. 221).

É necessário ter em conta que os objetivos de uma organização cobrem várias atividades, o que deve incluir riscos estratégicos, operacionais, financeiros, transparência, projetos, conformidade, dentre outros (Grumbach et al., 2020, p. 133).

Nesse sentido, o gerenciamento de riscos corporativos, para ser eficiente, deve levar em conta as estratégias, táticas e operações de finanças, marketing, recrutamento, contabilidade, tecnologia, e, claro, da área jurídica, principalmente quando a organização está sujeita à regulação estatal, ou mesmo às limitações ou condicionamentos contratuais com parceiros, clientes, fornecedores etc.

Assim, conforme avança o fenômeno de "digitalização do mercado", onde as organizações passam a ocupar espaços online e a depender essencialmente das Tecnologias de Informação e Comunicação (TIC) para existirem e operarem de maneira sustentável, torna-se necessário que os riscos pertinentes ao meio digital integrem a gestão em nível estratégico.

É essencial que todos os setores da organização estejam aptos a "identificar os riscos envolvidos em sua atividade, mensurá-los da forma mais objetiva possível, avaliar as consequências advindas da ocorrência de eventos desfavoráveis e favoráveis, avaliar possibilidades de mitigação desses riscos", e, a partir da análise sobre os custos e benefícios envolvidos, "acompanhar quanto esses riscos podem estar afetando ou afetarão negativamente os resultados da empresa e se podem representar uma perda significativa caso certas tendências prevaleçam" (Nakamura, sd, p. 222).

[9] Disponível em: Cetic.br — Centro Regional para o Desenvolvimento da Sociedade da Informação.

[10] E, justamente, o estabelecimento de políticas sobre segurança da informação pode minimizar as chances de danos a terceiros pelos prepostos da organização que utilizem de maneira indevida os recursos e ativos informacionais aos quais tiverem acesso em função do trabalho (Teixeira, 2018, p. 402).

[11] Por força da Lei nº 13.853, de 8 de julho de 2019, o início da vigência da LGPD foi postergado para 2020.

Por conseguinte, quanto mais departamentos e pessoas numa organização utilizam meios digitais para desempenhar sua função e, quanto mais dados pessoais são tratados nessas operações, cresce a necessidade de gerenciar os riscos de segurança digital espalhados por toda a estrutura organizacional, principalmente para prevenir os riscos advindos da LGPD.

Ao montar um modelo de gerenciamento de risco corporativo (ERM), a gestão da organização deve promover "uma visão holística de riscos e oportunidades, em que diferentes atividades e processos da empresa são analisados à luz dos riscos envolvidos e das oportunidades que podem ser aproveitadas", pois, de maneira geral, para todos os negócios, "o conceito de ERM é mais abrangente e envolve múltiplas abordagens" (Nakamura, sd, p. 222).

Enfim, toda essa apuração deixa ainda mais clara a necessidade de implementação de modelos de gestão de risco corporativo perante a regulação estabelecida pela LGPD, uma vez que, como visto, são incontáveis as atividades praticadas pelas organizações envolvendo dados de pessoas.

3. Gestão de Riscos e a Lei Geral de Proteção de Dados

De acordo com Grumbach et al. (2020, p. 138), a gestão de riscos deve entregar para a organização, dentre outros serviços, a conformidade com leis e regulamentos, e a garantia do gerenciamento dos riscos mais significativos.

Nesse sentido, dentre os vários tipos de riscos que uma organização precisa gerenciar, aqueles ligados à adequação de sua estrutura e seus processos à legislação de proteção de dados merece destaque, pois, como visto anteriormente, sua aplicabilidade é ampla no mercado, abrangendo seguramente todo tipo de organização — com maior ou menor grau de impacto.

Embora o processo do gerenciamento de riscos seja composto pelas etapas complementares de identificação, análise e avaliação dos riscos envolvidos, o presente estudo estará, por questão didática, limitado à primeira etapa (identificação de riscos).

Inicialmente, a identificação dos riscos de conformidade ligados à LGPD depende da análise das obrigações que ela prevê para as organizações e de sua consequência negativa em caso de descumprimento.

É necessário destacar, de antemão, que a lei não proibiu a utilização de informações pessoais pelas organizações, mas estabeleceu regras para que o tratamento seja considerado regular.

A definição do que seria o tratamento regular pode ser identificada, por exclusão, a partir daquilo que a lei considera como "irregular":

> "Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
>
> I — o modo pelo qual é realizado;
>
> II — o resultado e os riscos que razoavelmente dele se esperam;
>
> III — as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado".

Da previsão acima é possível destacar, pelo menos, duas instâncias de riscos a serem gerenciados: aqueles ligados à segurança dos dados e aqueles sobre a conformidade estrita à lei.

Quanto aos riscos de conformidade, uma das primeiras questões a serem avaliadas estaria na compreensão de que, a partir da LGPD, somente podem ser tratados dados de pessoas, pelas organizações, dentro das hipóteses legalmente autorizadas — o que se convencionou chamar de "bases legais":

> "Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I — mediante o fornecimento de consentimento pelo titular;
>
> II — para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III — pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV — para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V — quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI — para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII — para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII — para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> IX — quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X — para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente".

É necessário esclarecer que a LGPD considera que, em toda atividade com dados pessoais, estariam envolvidas duas figuras jurídicas descritas como "agentes de tratamento": o controlador, "a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI), e o operador, "que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII).

Assim, o primeiro risco relevante de conformidade a ser identificado diz respeito inclusive à forma como são, por exemplo, desenhados e executados os processos da organização que lidam com dados pessoais, obrigação que recai principalmente para aquela que for a controladora dos dados, responsável por administrar o tratamento.

Afinal, se, a partir da LGPD, o tratamento somente será considerado legítimo dentro de alguma das hipóteses autorizadas, então, os processos que se orientam pela coleta, uso e compartilhamento de dados pessoais, mas que não estiverem dentro das bases legais, oferecem riscos evidentes.

O segundo risco a ser apontado, ainda quanto aos requisitos legais, estaria nas regras para tratamento de dados sensíveis, categoria mais estrita de dado pessoal criada pela LGPD, que seria a informação sobre "origem étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político", ou "dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II).

Nesse sentido, como os dados sensíveis seriam aqueles ligados à intimidade do titular,[12] requerendo maior proteção, as hipóteses para sua utilização são mais restritas:

> "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I — quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II — sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

Outra seção de riscos estaria ligada ao tratamento de dados pessoais de crianças e adolescentes, população que recebe da legislação uma preocupação à parte, por se tratarem de pessoas presumidamente vulneráveis.

Nesse sentido, o art. 14 da LGPD traz uma série de condicionantes e limitações para a atuação do agente de tratamento em relação ao titular que seja menor de idade:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais

[12] Registre-se que a LGPD conceitua como titular "a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (art. 5º, V).

> e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Assim, como não poderá a organização lidar com os dados de menores da mesma forma que lida com os de outros titulares, existe um regramento específico para esse público e, consequentemente, existe aí outro risco de conformidade.

Por fim, quanto às regras sobre tratamento de dados, existe outra previsão na LGPD que deve ser observada pelas organizações, no que diz respeito especificamente ao término do tratamento:

> "Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I — verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II — fim do período de tratamento;
>
> III — comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei,[13] resguardado o interesse público; ou
>
> IV — determinação da autoridade nacional, quando houver violação ao disposto nesta Lei".

Por conseguinte, é necessário que todas as pessoas que participam dos processos com dados pessoais, em cada organização, estejam atentas para verificar a ocorrência de alguma das hipóteses que configuram o término do tratamento.

Até porque a própria LGPD determina que, após o término, os dados pessoais devem ser descartados pela organização:

> "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I — cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II — estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III — transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV — uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados".

Portanto, salvo nas hipóteses autorizadas acima, a organização que permanecer com os dados do titular estará realizando o tratamento de forma irregular, isto é, sem autorização legal.

Bom, como visto, há pelo menos 4 (quatro) tipos de riscos de conformidade relacionados aos requisitos do tratamento de dados pessoais e que precisam ser devidamente gerenciados de maneira sistêmica dentro da organização.

Outros riscos de conformidade podem ser identificados a partir das demais obrigações previstas na LGPD, como a necessidade de que o controlador nomeie publicamente o seu encarregado pelo tratamento de dados pessoais[14] (art. 41), que promova o atendimento aos direitos do titular[15] (art. 18), dentre outras regras.

Já quanto aos riscos de segurança, cumpre salientar que a própria LGPD prevê obrigações pertinentes que devem ser cumpridas pelas organizações:

> "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a 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".

A partir da leitura do texto legal, é possível perceber como toda organização deverá adotar, de forma orgânica e vinculada à sua estrutura operacional, medidas técnicas e gerenciais que se mostrem adequadas para prevenir qualquer tipo de tratamento acidental ou ilícito, se quiser minimizar os riscos de segurança digital.

Todavia, embora preveja essa espécie de obrigação, a LGPD não delimita nem conceitua quais os tipos de medidas que deverão ser adotadas, omissão que, ao mesmo tempo em que deixa margem de autonomia maior para que as próprias organizações definam como estruturar sua governança de informação, gera também insegurança do ponto de vista jurídico, pois a efetividade das medidas adotadas somente serão averiguadas no caso concreto.

[13] "Art. 8º. O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.[...] § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei".

[14] Encarregado é definido como "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (art. 5º, VIII).

[15] "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I — confirmação da existência de tratamento; II — acesso aos dados; III — correção de dados incompletos, inexatos ou desatualizados; IV — anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V — portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI — eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII — informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII — informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX — revogação do consentimento, nos termos do § 5º do art. 8º desta Lei".

Ou seja, uma organização que realiza o tratamento de dados pessoais somente será considerada segura enquanto não ocorrerem "acessos não autorizados" ou não acontecerem os incidentes de "destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Isso quer dizer que, de alguma maneira, o agente de tratamento saberá que suas medidas de segurança digital não eram eficazes, por exemplo, só depois que o incidente ocorrer, o que torna ainda mais necessário o gerenciamento dos riscos envolvidos.

Além disso, a LGPD também prevê explicitamente que "os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término" (art. 47).

Portanto, os riscos de segurança digital, longe de serem apenas uma questão ligada ao interesse gerencial da organização (para evitar ataques financeiros, perdas de propriedade intelectual, interrupção de serviços etc.), passam a ser reforçados pela LGPD como obrigação junto ao titular dos dados.

Até porque, além de o tratamento irregular ter como consequência as sanções administrativas mencionadas acima, a organização que causar algum prejuízo a terceiro durante o tratamento irregular, como visto, deverá responder pela indenização:

> "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

Assim sendo, a organização que não atuar em conformidade com a LGPD ou que não prover a devida segurança informacional poderá responder tanto perante a fiscalização (sanções administrativas) quanto perante aquele que for prejudicado (reparação de danos).

Certamente, caberá à administração da organização decidir qual o nível do risco de conformidade a ser tolerado em relação às questões levantadas, mas não se pode negar o impacto negativo que o descumprimento da LGPD e das medidas de segurança digital podem gerar.

Cumpre ressaltar, por fim, que a lei não propõe gradações para as punições a serem aplicadas, nem faz correspondência entre infrações e sanções, de modo que, em tese, o descumprimento de qualquer norma da lei pode ensejar qualquer uma das penalidades previstas no art. 52:

> "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;
>
> VII — (VETADO);
>
> VIII — (VETADO);
>
> IX — (VETADO);
>
> X — suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI — suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII — proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados".

Todavia, há previsão de alguns parâmetros e critérios a serem considerados na aplicação da sanção, levando em conta a postura da organização perante a lei, dentre os quais figura "a adoção de política de boas práticas e governança".[16]

"Boas práticas e governança" são termos aos quais a LGPD faz referência no seu art. 50, onde é estimulado que todas as organizações instituam o seu "programa de governança em privacidade".

[16]"Art. 52. [...] § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I — a gravidade e a natureza das infrações e dos direitos pessoais afetados; II — a boa-fé do infrator; III — a vantagem auferida ou pretendida pelo infrator; IV — a condição econômica do infrator; V — a reincidência; VI — o grau do dano; VII — a cooperação do infrator; VIII — a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX — a adoção de política de boas práticas e governança; X — a pronta adoção de medidas corretivas; e XI — a proporcionalidade entre a gravidade da falta e a intensidade da sanção".

Comumente conhecido como programa de compliance de dados, sua adoção deve cumprir alguns requisitos previstos na lei (art. 50, § 2º, I) para que seja considerado como efetivamente instituído.

Em primeiro lugar, deve evidenciar a adoção de processos e políticas internas que assegurem o cumprimento das normas e boas práticas relativas à proteção de dados pessoais (art. 50, § 2º, I, "a").

Ademais, deve ser aplicável a todo o conjunto dos dados pessoais que estão sob controle da organização, sendo adaptado à estrutura, à escala e ao volume de suas operações (art. 50, § 2º, I, "b" e "c").

Políticas e salvaguardas adequadas, baseadas em processo de avaliação sistemática de impactos e riscos à privacidade, devem também ser adotadas pela organização, contando com planos de resposta a incidentes (art. 50, § 2º, I, "d" e "g").

Ademais, o programa deve ser objeto de monitoramento contínuo e avaliações periódicas, o que deve se revelar na sua constante atualização (art. 50, § 2º, I, "h").

Tudo isso converge para que seja demonstrado o objetivo central de estabelecer uma relação de confiança com o titular dos dados, por meio de atuação transparente da organização (art. 50, § 2º, I, "e").

E, por fim, nada disso será possível, contudo, se o programa não estiver integrado à estrutura geral de governança da organização, com mecanismos efetivos de supervisão internos e externos (art. 50, § 2º, I, "f").

Portanto, como se pode ver, embora não seja de adoção obrigatória, o programa de compliance de dados é essencial para as organizações que pretendem efetivar a gestão de riscos em nível estratégico (ERM).

Afinal, a sua adoção somente será considerada como efetiva, funcionando assim como parâmetro a ser considerado na aplicação de penalidades, de modo a minimizar os impactos negativos do risco de conformidade, se estiver integrado à sua estrutura geral de governança.

A principal função dos programas de compliance, no âmbito da proteção de dados pessoais, seria obviamente auxiliar no atendimento aos comandos legais,[17] mas de acordo com a realidade particularmente vivenciada pelo agente de tratamento, que passa a contar com orientações técnicas e administrativas prontamente identificáveis, prevenindo na sua atuação violações aos direitos dos titulares (Frazão et al., 2019, p. 682).

Ademais, o amplo escopo de incidência da LGPD torna necessária análise de conformidade não apenas das atividades-fins, mas de qualquer operação ou procedimento interno das organizações que tratam dados pessoais (Frazão et al., 2019, p. 695), o que enaltece o papel do programa de compliance de dados para a adequada gestão de riscos.

Portanto, o programa de governança em privacidade previsto na LGPD pode não apenas minimizar os impactos negativos do seu descumprimento, por servir como parâmetro de calibração na aplicação das sanções administrativas, mas funcionar, por si só, como ferramenta adequada para a gestão dos próprios riscos de segurança e conformidade da organização na lida com dados pessoais.

4. Conclusões

Consoante visto ao longo do estudo, o gerenciamento de riscos digitais tem se revelado um dos desafios mais críticos para a maioria das organizações.

Conforme cresce o nível de atuação das organizações em ambientes digitais, aumenta também a probabilidade de impactos negativos advindos da falta de segurança das informações e dados por elas gerenciados.

E, a partir da Lei Geral de Proteção de Dados, os riscos envolvidos com a segurança da informação passam a ter uma dimensão que vai além dos impactos econômicos (ativos, marca etc.), abrangendo agora o risco de penalizações administrativas e responsabilização judicial por danos.

Essa é uma realidade que precisa ser enfrentada de maneira adequada, para não inviabilizar a própria atividade econômica, seja com o atravancamento das operações pelo excesso de restrições, seja pelos impactos negativos que podem advir justamente da ausência de controles.

Mas como visto, sequer a adoção de políticas de segurança digital é uma realidade para a maioria das organizações brasileiras, o que, por outro lado, revela a relevância e o potencial que a LGPD apresenta para estimular a adoção de boas práticas e padrões de segurança da informação.

Essa é uma tarefa complexa, pois, de um lado, dados pessoais costumam circular por praticamente toda a estrutura das organizações, de maneira pulverizada, em vários ambientes (correio eletrônico, sistemas de terceiros, bancos de dados, servidores internos etc.), o que aumenta os riscos de segurança digital, e, de outro, são diversas as regras estabelecidas pela legislação, que devem ser observadas em cada uma dessas atividades que envolvem dados pessoais, o que destaca os riscos de conformidade.

O gerenciamento desses riscos deve ser realizado de maneira conjunta, pois a própria LGPD prevê obrigações de segurança digital que devem ser cumpridas pelos agentes de tratamento, o que tende a impactar suas estruturas, processos e relacionamentos quanto à privacidade e proteção de dados.

Nesse ponto, deve se destacar que o "programa de governança em privacidade" previsto na própria LGPD pode funcionar como adequado instrumento para estruturação da ERM na organização, pois, além de a sua execução contar com vários processos de gerenciamento de riscos de conformidade e segurança, a sua adoção, por si só, já configura uma ferramenta para minimizar os impactos das sanções administrativas.

[17] Programas de compliance auxiliam na identificação, análise e avaliação de riscos, permitindo a atuação preventiva contra o cometimento de ilícitos, evitando demandas administrativas ou judiciais para corrigir algum desvio (Crespo e Bagnoli, 2020, p. 458).

Referências

Albani, A. H. S. (2019). Disposições preliminares. In Feigelson, B. e Albani, A. H. S., editors, *Comentários à lei geral de proteção de dados*. Thomson Reuters, São Paulo.

Cantoni, S., Lins, L., e Jereissati, T. (2020). *Segurança digital e gestão de riscos: uma análise de empresas brasileiras*. Comitê Gestor da Internet no Brasil, São Paulo.

CGI.br, Comitê Gestor da Internet no Brasil (2019). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2018*. CGI.br, São Paulo.

CGI.br, Comitê Gestor da Internet no Brasil (2020). *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação (TIC) no mercado brasileiro: TIC Empresas 2019*. CGI.br, São Paulo.

Crespo, L. C. e Bagnoli, V. (2020). O papel do compliance no mercado que comercializa dados. In Saavedra, G., editor, *Governança corporativa, compliance e gestão de riscos*. ESENI, São Paulo.

Crespo, M. e Camargo, C. A. (2018). Transformação digital no cenário internacional. In Pinheiro, P. P., editor, *Direito digital aplicado 3.0*. Thomson Reuters, São Paulo.

Frazão, A., Oliva, M. D., e Abilio, V. d. S. (2019). Compliance de dados. In Tepedino, G., Frazão, A., e Oliva, M. D., editors, *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. Revista dos Tribunais, São Paulo.

Grumbach, R. J. d. S., Franco, F. L., Silva, J. W. d., e Grumbach, R. P. (2020). *Construindo o futuro: o método Grumbach de gestão estratégica*. Cia do eBook. Edição do Kindle.

Nakamura, W. T. (s.d.). *Gestão: controle interno, risco e auditoria*. Saraiva. Edição do Kindle.

OCDE (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. OCDE, Paris.

Teixeira, T. (2018). *Curso de direito e processo eletrônico*. Saraiva, São Paulo, 4 edition.