CONFORME:
Lei 14.010/2020
Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado no período da pandemia de Covid-19

Coordenação:
Tarcisio Teixeira

Organização:
André Pedroso Kasemirski
Rodolfo Ignácio Aliceda

EMPRESAS E IMPLEMENTAÇÃO DA LGPD

– Lei Geral de Proteção de Dados Pessoais

2021

EDITORA JusPODIVM
www.editorajuspodivm.com.br

2

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E *DATA MAPPING* (MAPEAMENTO DE DADOS): DESAFIOS, PERSPECTIVAS E COMO SE ADEQUAR À NOVA LEI NA PRÁTICA

Tatiana Kolly Wasilewski Rodrigues[1]

INTRODUÇÃO

Na segunda metade do século XX a indústria tradicional passou a valorizar a informação e a tecnologia em maior escala, o que modificou o espaço geográfico global, e posteriormente culminou no advento da Terceira Revolução Industrial, também conhecida como a Era da Informação.

1 Especialista em Direito e Processo do Trabalho. Advogada. tatiwr@gmail.com.

A tecnologia da informação está produzindo profundas modificações nos espaços públicos e privados, modificando a própria ciência jurídica que tenta regulamentar e coibir os impactos tecnológicos negativos experimentados e que se tornaram grandes desafios para o Direito, o que passou a exigir respostas rápidas e eficazes no que tange este novo fenômeno.

Nessa nova etapa da sociedade industrial e da evolução histórica dos direitos humanos, a dignidade da pessoa humana perpassa pela proteção dos dados pessoais, em especial pelos dados sensíveis, o que propiciou a criação de hodiernos regimes jurídicos que passaram a tutelar de modo mais rigoroso e pedagógico a coleta, armazenamento, tratamento, processamento, proteção e o sigilo desses dados.

Além de invadir a privacidade e violar a dignidade dos titulares de dados pessoais, os problemas que decorrem da exploração indevida das informações privadas e públicas podem ocasionar danos irreversíveis à imagem e a reputação dessas corporações e instituições, podendo levar até inviabilidade da atividade econômica das empresas responsáveis pelo tratamento desses dados.

Assistiu-se nos últimos anos à promulgação de regulamentos destinados a construção de uma cultura de proteção da informação, em especial pela União Europeia, que no ano de 2016 aprovou um importante instrumento de tutela desses dados, o *General Data Protection Regulation* (GDPR).

Na "desventurosa" condição de líder em violação de dados na América Latina, o Brasil aprovou recentemente um importante aliado para resguardar tutelar a segurança da informação, que objetiva balizar as relações em um contexto de relações digitais sem fronteira. Fortemente inspirada na GDPR a Lei n. 13.709/2018, popularmente conhecida como Lei Geral de Proteção de Dados Pessoais, estabelece rígidos regramentos quanto a sua gestão.

A LGPD traz uma série de exigências e regulamentações para as empresas, o que exige grandes mudanças por parte das de todos os atores empresariais responsáveis pela gestão da informação, e ao considerar como

responsáveis pelos vazamentos de informações as empresas encarregadas da gestão e proteção de dados, a LGPD prevê duras penalidades, o que leva muitas empresas a implementarem de forma equivocada medidas exclusivamente voltadas a prevenção de uma eventual responsabilização penal e administrativa, esquecendo-se de concretizar processos e técnicas adequados à proteção dos dados privados e a redução dos riscos.

A LGPD não foi criada para limitar a atuação das empresas gestoras de dados e sim para promover a inovação, bem como a expansão segura dessas atividades, tendo por missão a proteção e promoção dos direitos fundamentais, essenciais para efetiva tutela dos dados privados de seus cidadãos, de seus instituições e corporações privadas.

Nesse quadro, o direito aliado a tecnologia e a multidisciplinariedade viabilizaram o surgimento de relevantes soluções que possibilitam o fiel cumprimento da legislação que disciplina a matéria de proteção de dados, todavia estes métodos e procedimentos exigem muitas vezes uma mudança radical na forma de como a empresa lida com o tratamento de dados pessoais.

Em razão de ser uma tema recente no Brasil, os métodos que auxiliam no processo de adequação as legislações de proteção de dados são encontrados de forma limitada e superficial, com a edição de poucas doutrinas que abarcam de forma aprofundada a matéria, todavia a partir de uma interpretação analógica da LGPD, assim como da importação de métodos bem-sucedidos de países que possuem certa solidez e adaptação a legislação pertinente, dessa forma, o presente artigo abordará os principais mecanismos que auxiliam no correto gerenciamento da informação, e assim do processo de adequação a Lei Geral de Proteção de Dados (LGPD).

O *compliance*, as boas práticas de governança, o gerenciamento de riscos, o plano emergencial para incidente de vazamento de dados e de forma especial o mapeamento de dados, são indispensáveis para a garantia da segurança e a proteção das informações, e são algumas das mais variadas técnicas de adequação a LGPD.

Considerado o primeiro passo a ser dado por qualquer organização ao iniciar o processo de adequação a LGPD, será concedido o devido enfoque ao mapeamento de dados no presente artigo, essa é uma solução tecnológica que possibilita uma visão ampla e aprofundada do quadro de dados controlados pelas empresas, e que favorece a segura introdução de outros métodos essenciais ao processo de adequação a Lei Geral de Proteção de Dados.

Dessa forma, os impactos da recente base legal regulatória acabam por adequar essas corporações as novas transformações do mercado global, onde o comprometimento com a segurança e o sigilo da informação não são mais um *plus* nas ofertas de serviços, e sim requisitos integrantes e essenciais no tratamento desses dados.

Salientada a magnitude do tema proposto, cabem às ponderações colocadas no decorrer do desenvolvimento da pesquisa para promover contribuições no sentido de proporcionar respostas e soluções aos percalços e desafios a serem enfrentados pelas empresas de economia digital, face o advento da nova Lei Geral de Proteção de Dados.

1. OS DIREITOS TUTELADOS PELA LEI GERAL DE PROTEÇÃO DE DADOS

Previstos anteriormente em esparsos dispositivos legais, tais como a Constituição Federal, o Código Civil e de Defesa do Consumidor, a Lei de Acesso à Informação e do Cadastro Positivo e o Marco Civil da Internet, a tutela de dados pessoais no Brasil era na conflituosa na prática, diante das contradições encontradas nos diferentes dispositivos que disciplinaram a matéria, o que gerava uma certa insegurança jurídica[2].

2 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 71-74.

Acompanhando a necessidade do mercado e da tendência mundial, a Lei Geral de Proteção de Dados criada no ano de 2018 passou a disciplinar e proteger de forma eficiente e rigorosa o tratamento de dados pessoais no Brasil, estipulando pesadas sanções para quando for constatado violações a essas regulamentações.

Prevista para entrar em vigor apenas no ano de 2021, a LGPD pode ser vista como um obstáculo as empresas controladoras de dados pessoais que se fundam na exploração da atividade econômica de forma predatória e irresponsável ao considerarem os dados sensíveis como simples bens patrimoniais[3].

A nova Lei Geral de Proteção de Dados se baseia nos direitos fundamentais de liberdade e privacidade, tendo como missão a transformação das práticas e dos negócios digitais. Nesse sentido, é importante destacar que a lei não foi criada para limitar a atuação das empresas gestoras de dados e sim para promover a inovação e a expansão segura dessas atividades.

Nesse cenário, é fundamental destacar os conceitos de dados pessoais e sensíveis apresentados pela LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II – dado pessoal sensível: dado pessoal sobre origem racial ou 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.

3 MENDES, Laura Schertel. **Privacidade, Proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 122-123.

De forma especial, a LGPD firma seu compromisso na tutela de dados pessoais, e de forma mais específica com os dados sensíveis. Existem considerações probabilísticas de que tais dados são mais afeitos a apresentarem problemas "mais graves quando de sua má utilização – daí exatamente o fato de denominá-los como 'sensíveis' em relação aos demais, enfatizando sua peculiaridade neste sentido"[4]. Por essa razão, vez que podem ensejar alto potencial lesivo ao seu titular, a LGPD atribuiu uma elevada proteção aos dados particulares, e de modo especial as sensíveis.

Ao prever em seus artigos iniciais como escopo os direitos fundamentais, dignidade de seus titulares e de seus consumidores, a LPGPD reforça seu compromisso na tutela de dados pessoais:

> 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.
>
> [...]
>
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;

4 DONEDA, Danilo. **Privacidade e transparência no acesso à informação pública**. Zaragoza: Prensas Universitarias de Zaragoza, 2010. p. 179-216.

> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Mais à frente, a LGPD elenca no artigo 6º, de modo exemplificativo, um rol de princípios a serem observados nas atividades de tratamento de dados pessoais, são eles: o princípio da boa-fé objetiva; da finalidade; da necessidade; do livre acesso; da qualidade dos dados; da transparência; da segurança; da prevenção; da não discriminação; e o princípio da responsabilização e prestação de contas.

Como se pode observar, fica clara a preocupação da LGPD em conferir proteção ao titular dos dados sensíveis, essa proteção consiste em um autêntico direito fundamental, sendo expressão dos direitos da personalidade, em especial da privacidade, do sigilo e propriamente até da estabilidade democrática, vez que esses direitos estão "intrinsecamente relacionados à impossibilidade de transformar os indivíduos em objeto de vigilância constante", em especial dos controladores de dados preocupados unicamente em colocar seus lucros acima de qualquer outro valor[5].

2. OS PRINCIPAIS RISCOS DE NÃO SE ADAPTAR À LGPD

Com o propósito de tutelar de forma eficiente os dados pessoais, visando a coleta, proteção, armazenamento, tratamento e transferência segura dos dados pessoais, a LGPD estipulou pesadas punições para aqueles que descumprirem suas determinações. De forma clara e específica, a

5 FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. São Paulo: Revista dos Tribunais, 2019, p.100.

LGPD discriminou quem são os atores envolvidos no processo de tratamento de dados, bem como suas atribuições, responsabilidades e possíveis penalidades, não restringindo sua aplicação exclusivamente as empresas de tratamento de dados.

> Ao contrário do que parece, a LGPD não se aplica apenas a empresas do segmento de tecnologia, mas a qualquer uma, tanto no setor público quanto no privado, que colete dados de seus usuários. Isso quer dizer que instituições bancários, cadastros de condomínio e até algumas páginas do Facebook deverão se adequar à nova lei de proteção de dados caso não queiram sofrer as sanções[6].

É notório que a LGPD protege direitos individuais e nesse aspecto não faz sentido que a lei esteja vigente sem disciplinar com seriedade e poder de coerção uma matéria tão cara aos cidadãos, as corporações e as instituições brasileiras.

Segundo o regulamento da lei que dispõe sobre a proteção de dados no Brasil, os agentes de tratamento da informação que violarem as normas por ela estabelecidas, ficam sujeitos a sanções administrativas que variam de simples advertências a pesadas multas que podem levar rapidamente ao fim da atividade empresarial, de modo particular das empresas de pequeno porte que tenham a infelicidade de sofrer sucessivos vazamentos de dados pessoais[7].

---

6 SILVA, Rafael Rodrigues da Silva. **Multa de R$ 50 milhões será aplicada às empresas que não se adequarem à LGPD**. 10 de out. de 2020. Disponível em: https://canaltech.com.br/legislacao/multa-de-r-50-milhoes-sera-aplicada-as-empresas-que-nao-se-adequarem-a-lgpd-124552/. Acesso em 09 de jun. de 2020.

7 JUNIOR, Sebastião Ventura Pereira da Paixão. **Lei Geral de Proteção de Dados: sanções, pedagogia e o dilema do futuro**. 25 de dez. de 2019. Disponível em:https://www.conjur.com.br/2019-dez-25/sebastiao-ventura-lgpd-sancoes-pedagogia-dilema-futuro. Acesso em 08 de jul. de 2020.

O artigo 52 da LGPD engloba um rol de sanções que se aplicam a qualquer forma de descumprimento das regulamentações, práticas e condutas por ela assentada, sendo aplicadas somente após procedimento administrativo que possibilite a oportunidade da ampla defesa, nos termos do §1º do artigo 52, sendo igualmente observados quando da aplicação da penalidade a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem econômica auferida pelo infrator; sua condição econômica; a reincidência; o grau do dano; a cooperação do infrator; a adoção demonstrada de mecanismos e procedimentos internos capazes de minimizar os danos, assim como a adoção de políticas de boas práticas e governança.

Os incisos do artigo 52 elencam precisamente 08 (oito) sanções administrativas a serem aplicadas em razão de infrações que violem a LGPD, sendo: advertência, com indicação acompanhada de prazo para adoção de medidas corretivas; multa simples, que pode chegar até 2% (dois por cento) do faturamento da pessoa jurídica, grupo ou conglomerado econômico, limitada no total em R$ 50 milhões (cinquenta milhões de reais) por infração; multa diária, novamente limitada a R$ 50 milhões; a publicização da infração, somente após o procedimento administrativo que tenha possibilitado a oportunidade da ampla defesa e que tenha assim restado comprovado o ilícito; o bloqueio, bem como a eliminação dos dados pessoais a que se refere a infração; a suspensão temporária por até 06 (seis) meses do funcionamento do banco de dados relacionado com a infração, com a possibilidade de ser prorrogado por igual período; e por fim a proibição total ou parcial do exercício da atividade relacionada a tratamento de dados pessoais.

Uma novidade em relação as penalidades impostas pela Lei Geral de Proteção de Dados é a possibilidade de pactuação de acordo de conciliação entre o titular dos dados e da empresa responsável por seu tratamento, caso seja comprovada a responsabilidade do controlador na quebra da segurança e sigilo da informação. Caso não seja possível uma conciliação

entre as partes envolvidas, a contratada fica sujeita as sanções previstas pelo novo Código de Defesa da Privacidade[8].

Malgrado as severas punições estipuladas, elas são indispensáveis para uma efetiva tutela de proteção de dados e até mesmo para o desenvolvimento das relações comerciais empresariais, visto que uma resposta branda do poder regulatório frente violações a norma, tornaria a LGPD inócua, o que evitaria a promoção da competividade e do consequente fortalecimento da atividade econômica no setor. Nesse sentido pontua a Associação das Empresas Brasileiras de Tecnologia da Informação de São Paulo (ASSESPRO-SP):

> De acordo com a Associação [...], a LGPD é uma necessidade para o setor, pois protege usuários e cria um padrão para que todas as instituições possuam as mesmas responsabilidades e encargos quanto às informações coletadas, o que irá facilitar as trocas comerciais internacionais.
>
> [...] Um dos principais perigos para esses dados é a ação de cibercriminosos, já que, além de prejuízos à imagem da empresa, o roubo de dados em invasões pode também acarretar em multas sob a nova lei.
>
> Para eliminar esse problema [...] é necessário que as empresas tomem medidas práticas, como avaliação das estruturas de rede e aplicações de testes de intrusão, além da

8 FARIA, Wiliam. LGPD: **O que mudou na redação final da lei? Sanções da LGPD**. 14 de out. de 2019. Disponível em: https://canaltech.com.br/legislacao/lgpd-o-que-mudou-na-redacao-final-da-lei-152367/#:~:text=San%C3%A7%C3%B5es%20da%20LGPD&text=Multa%20di%C3%A1ria%2C%20observado%20o%20limite,infra%C3%A7%C3%A3o%20at%C3%A9%20a%20sua%20regulariza%C3%A7%C3%A3o%3B&text=Essas%20puni%C3%A7%C3%B5es%20existentes%20na%20Lei,para%20sua%20adequa%C3%A7%C3%A3o%20%C3%A0%20LGPD. Acesso em 09 de jul. de 2020.

> renovação de políticas de segurança e modernização dos aplicativos utilizados[9].

Portanto, a promoção de técnicas e procedimentos aptos a colocar em conformidade a atividade empresarial nos ditames da LGPD é essencial para o fortalecimento da atividade econômica e da própria sobrevivência da empresa em um mercado cada vez mais competitivo.

3. IMPORTANTES FERRAMENTAS DE ADEQUAÇÃO A LGPD

A ciência tradicional do Direito já não é capaz de tutelar as relações humanas nos ambientes digitais, dessa forma surgiu uma nova ramificação entre o Direito e a tecnologia, capaz reger as relações em ambientes virtuais de forma a estabelecer leis e garantir que ninguém seja lesado nesse campo. Com a vigência das leis de proteção de dados, a gestão da informação se torna cada vez mais importante, desse modo, e de forma ampla e irrestrita a interdisciplinaridade surge como peça fundamental para a construção e a consequente solidificação dessas novas práticas[10].

A aliança entre Direito e tecnologia não se restringe a tutela Estatal, o domínio da gestão dos dados se tornou uma tarefa cada vez mais importantes para as corporações, sejam elas públicas ou privadas, e nesse contexto surgem mecanismos que auxiliam no processo de gerenciamento da informação e na correta adequação a Lei Geral de Proteção de Dados (LGPD):

---

9 SECURITY REPORT. **Multa de R$ 50 milhões por infração poderá ser paga por descumprimento à LGPD**. 11 de out. de 2018. Disponível em: https://www.securityreport.com.br/overview/multa-de-r-50-milhoes-por-infracao-podera-ser-paga-por-descumprimento-a-lgpd/#.XwdmeyhKjIU. Acesso em: 09 de jun. de 2020.

10 SOLOMON, Robert C. **Ética e excelência: cooperação e integridade nos negócios**. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Civilização Brasileira, 2006. p. 24.

o *compliance*, as boas práticas de governança, o gerenciamento de riscos, o plano emergencial para incidente de vazamento de dados e de forma primordial o mapeamento de dados[11], que será abordado mais a frente.

3.1. *Compliance*

Advindo do verbo em inglês *to comply*, *o compliance* é um método que vem se popularizando no Brasil, em especial com a chegada da LGPD. Amplamente conhecido e aplicado em transparentes, éticas e renomadas corporações, o *compliance* objetiva reduzir os riscos da atividade empresarial, se voltando para "concretização da missão, da visão e dos valores de uma empresa"[12].

Como bem assinala a professora e advogada Ana Paula Candeloro, o *compliance* não pode ser compreendido apenas como um mero e corriqueiro cumprimento de normas externas e internas, veja-se:

> O *compliance* se caracteriza como um conjunto de regras, padrões, procedimentos éticos e legais, que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como a atitude dos seus funcionários[13].

Desse modo o *compliance* se caracteriza como método responsável pela manutenção e controle dos riscos legais, com procedimentos

---

11 GONÇALVES, José Antônio Pereira. **Alinhando processos, estrutura e compliance à gestão estratégica**. São Paulo: Atlas, 2012. p. 125.

12 DINIZ, Patrícia Dittrich Ferreira; Ribeiro, Márcia Carla Pereira. ***Compliance* e Lei Anticorrupção nas empresas**. Revista de Informação Legislativa, Brasília, DF. Ano 52, Número 205, jan./mar. 2015. p. 88.

13 CANDELORO, Ana Paula; RIZZO, Maria Balbina Martins de; PINHO, Vinícius. ***Compliance* 360º: riscos, estratégias, conflitos e vaidades no mundo corporativo**. São Paulo: Trevisan Editora Universitária, 2012. p. 154.

especificamente direcionados a garantir a conformidade dos regulamentos legais nacionais e internacionais, além dos regramentos internos.

Em suma, essa prática se aplica a todos os tipos de instituições e envolve uma conduta essencial no mercado atual, visto a exigência de condutas legais cada vez mais rígidas e punitivas, dada a relevância dos direitos tutelados, em especial da LGPD[14].

Verifica-se assim a importância dada pela lei ao *compliance*, sendo sua implementação essencial para o desenvolvimento da empresa, da transparência, da ética e da sociedade, servindo assim como instrumento efetivo de construção e consolidação da LGPD.

3.2. Boas Práticas de Governança

A LGPD prevê de modo específico em seu artigo 50 e seguintes as boas práticas e condutas de governança que visam adequar as atividades das empresas controladoras de dados ao que dispõe os direitos por ela tutelados.

O referido dispositivo permite que as corporações que exercem atividades econômicas que envolvem tratamento de dados criem regras de boas práticas e de governança, desde que estabeleçam, por exemplo, condições de organização, regimes de funcionamento, procedimentos, normas de segurança e de padrões técnicos, mecanismos internos de supervisão e de mitigação de riscos, e outros aspectos relacionados ao tratamento das informações sensíveis[15].

---

14 ROONEY, Allan. **Effective Data Mapping and GDPR Compliance**. Disponível em: https://www.forbes.com/sites/entrepreneursorganization/2018/11/01/effective-data-mapping-and-gdpr-compliance/#6c673920421b. Acesso em 15 de jun. de 2020.

15 PLUGAR. **Conheça as boas práticas de governança e sanção da LGPD**. 30 de maio de 2019. Disponível em: https://www.plugar.com.br/conheca-as-boas-praticas-de-governanca-e-sancao-da-lgpd/. Acesso em 20 de jun. de 2020.

Segundo o manual da Associação Brasileira de Anunciantes (ABA) para adequação a LGPD, um programa de boas práticas de governança em privacidade deve:

> a. demonstrar o comprometimento da empresa 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. ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;
>
> c. ser adaptado à estrutura, à escala e ao volume das operações da empresa, bem como à sensibilidade dos dados tratados;
>
> d. estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
>
> e. ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
>
> f. estar integrado a sua estrutura geral de governança de forma a estabelecer e aplicar mecanismos de supervisão internos e externos;
>
> g. contar com planos de resposta a incidentes e remediação; e
>
> h. ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas[16].

Nesse contexto, a aplicação das boas práticas de governança é indispensável para a efetividade da LGPD e assim da tutela dos direitos

16 ASSOCIAÇÃO BRASILEIRA DE ANUNCIANTES. **Manual ABA para adequação à LGPD: Orientações e boas práticas de governança de dados para publicitários**. Disponível em: http://www.aba.com.br/wp-content/uploads/2019/06/ebook-aba-compliance-lgpd.pdf. Acesso em: 02 de jul. de 2020.

individuais, o que torna imperiosa a necessidade de mudanças com o fito de adequar as empresas aos ditames do que estabelece a legislação. Novamente, uma vez instituídos esses métodos, as corporações que exercem a exploração da atividade econômica no setor da informação podem construir uma boa reputação e se consolidarem de forma rápida em seu nicho.

3.3. Gerenciamento de Riscos

A falha e/ou a ausência de um processo de gestão de riscos torna a empresa responsável pela gestão de dados vulnerável a graves consequências, o que pode acarretar incertezas e prejuízos irreversíveis. Em resposta a esse problema surge o gerenciamento de riscos, processo esse que planeja, organiza, dirige e controla toda a cadeia produtiva de uma organização, objetivando reduzir ao máximo ou aproveitar as incertezas sobre essa organização[17].

Ao prever impactos e antecipar procedimentos que possam minimizar possíveis falhas capazes de inviabilizar o prosseguimento da atividade econômica, e assim como estimular novos procedimentos de proteção e segurança de dados, consoante dispõe a LGPD, o gerenciamento de riscos se estabelece como um grande aliado no cumprimento da referida legislação, e de forma especial quando da elaboração do Relatório de Impacto à Proteção dos dados pessoais, veja-se:

> [...] sua elaboração é um exercício fundamental para que a instituição tenha ampla visão de seu modelo de negócio e, assim, consiga averiguar eventual falha em seu fluxo de dados e/ou tomar decisões mais assertivas no

17 OLIVEIRA, WALLACE. **O que é gerenciamento de riscos? Finalidades e conceito**. 29 de nov. de 2014. Disponível em: https://www.venki.com.br/blog/o-que-e-gerenciamento-de-riscos/. Acesso em 17 de jun. de 2020.

> desenvolvimento de novos produtos ou serviços. Além disso, em caso de eventual auditoria ou processo administrativo perante a Autoridade Nacional, essa documentação poderá servir como base para demonstrar a boa-fé, a diligência e o comprometimento da instituição em termos de governança, conformidade com a legislação e preocupação com a segurança e sigilo dos dados pessoais dos titulares e, por conseguinte, atenuar eventual sanção administrativa[18].

Nesse sentido, apesar de não ser obrigatória a elaboração do Relatório de Impacto à Proteção dos dados pessoais, o referido procedimento quando adotado como prática na gestão de riscos, abarcando todo esse gerenciamento, pode significar o tratamento eficaz contra as incertezas que eventualmente se concretizam em perdas e prejuízos, assim como minimizar o efeito delas caso o risco se concretize.

3.4. Plano Emergencial para Incidente de Vazamento de Dados

A LGPD revela grande preocupação com a segurança e o sigilo dos dados, de modo especial no capítulo VII, seção I, ao estabelecer a necessidade dos controladores em caso de incidente de segurança que possa acarretar potencial risco ou dano relevante aos titulares, de adotarem uma série de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais.

Em caso de vazamento de dados, as empresas responsáveis pela segurança e gestão desses dados devem atender com velocidade os comandos da

18 DANIEL. **Conhecendo a Lei Geral de Proteção de Dados do Brasil: LGPD**. Fev. de 2019. Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em 10 de jul. de 2020.

LGPD, de forma a evitar maiores prejuízos aos direitos individuais, coletivos e até mesmo da própria atividade empresarial[19]. O planejamento emergencial previamente elaborado pelo quadro técnico que abarca esse tido de situação demostra o compromisso social da empresa, sua preocupação com a defesa e proteção dos dados que manipula, o que evita maiores prejuízos aos direitos individuais, coletivos e a aplicação de sanções que possam comprometer a própria continuidade da atividade empresarial[20].

4. MAPEAMENTO DE FLUXO DE DADOS PESSOAIS E LGPD: COMO INICIAR O TRATAMENTO DE DADOS COM SEGURANÇA NA PRÁTICA

A bem-sucedida implementação da LGPD é resultado inicialmente do compromisso com a alta administração, o que engloba tecnologia e interdisciplinaridade. Nesse contexto surge um dos mais importantes métodos de adequação ao novo Código de Defesa da Privacidade, o mapeamento de dados, figura essa que permite demostrar de que forma a corporação responsável pela gestão de dados pessoais está lidando com a privacidade e segurança da informação de seus titulares[21], bem como possibilitar a aplicação e o consequente êxito de outros procedimentos direcionados a garantir a conformidade da atividade empresarial com os ditames da LGPD, a exemplo dos métodos de adequação anteriormente explanados.

---

19 CERQUEIRA, Saulo. **LGPD e plano de contingência no vazamento de dados**. 17 de fev. de 2020. Disponível em: https://www.anyconsulting.com.br/lgpd-e-plano-de-contingencia-no-vazamento-de-dados/. Acesso em 09 de jun. de 2020.

20 GONZÁLEZ, Mariana. **O que é e como organizar um plano de contingência de TI**. 1º de out. de 2019. Disponível em: https://blog.idwall.co/plano-de-contingencia-de-ti/. Acesso em 09 de jun. de 2020.

21 PINHEIRO, Patrícia Peck Garrido**. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas**. São Paulo: Revista dos Tribunais, 2019. p. 74-76.

> Um dos principais objetivos do mapeamento de dados é diagnosticar a forma como a empresa lida com a privacidade e a segurança da informação de seus clientes, colaboradores e parceiros terceirizados, cumprindo, desta forma, a exigência constante no art. 37 da LGPD onde estipula que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem[22].

Dessa forma, o mapeamento de dados torna-se imprescindível as empresas controladoras de dados pessoais, vez que o processo dará um panorama geral de como a empresa trata e lida com a privacidade e a segurança dos dados, cumprindo assim com o disposto no artigo 37 da LGPD.

O mapeamento de dados, também conhecido como inventário de dados, *data mapping* ou ainda *data flow*, como destacado, trata-se de um documento essencial no processo de adequação a legislação que tutela a proteção de dados no Brasil. O referido documento deve refletir o método e o processo pelo qual foi submetido os dados pessoais dentro da corporação, o que incluí os processos e procedimentos pelos quais o dado transita, desde sua origem, "a base legal que respalda, o nível de segurança da base de dados a qual o dado pertence, entre outras informações necessárias para a análise de vulnerabilidades técnicas e jurídicas".

O *data mapping* é uma solução tecnológica que possibilita a empresa responsável pelo tratamento de dados uma visão ampla e aprofundada de como ela lida com o processo de gestão, tratamento e segurança desses dados, de modo que consiga identificar de forma ágil a origem e a fonte

22 BRANDÃO, Graziela. **O que é mapeamento de dados**. 27 de fev. de 2020. Disponível em: https://blconsultoriadigital.com.br/mapeamento-de-dados/#:~:text=O%20que%20%C3%A9%20o%20mapeamento%20de%20dados%3F&text=O%20mapeamento%20de%20dados%2C%20ou,LGPD%2C%20GDPR%2C%20CCPA). Acesso em 02 de jul. de 2020.

desses dados, assim como e com quem eles são compartilhados, entendendo todos os processos e fases de seu ciclo dentro da corporação, como bem pontua Luísa Varella:

> O mapeamento dos dados pessoais é a principal ação a ser tomada na sua gestão de riscos. Ele envolve tanto os dados de clientes quanto os de colaboradores e é o que vai garantir que a sua empresa está em conformidade com a lei.
>
> Esse processo tem como objetivo identificar quais dados estão em posse da empresa e assegurar sua privacidade dos dados, salvaguardando empresas que porventura possam vir a enfrentar problemas como vazamentos, denúncias e afins.
>
> A adequação pode ser um processo demorado, dependendo do estágio de aderência da empresa à Lei Geral de Proteção de Dados, mas é imprescindível[23].

À vista disso, é primordial conhecer o modo como a informação é recebida, criada, armazenada, processada e acessada e quais os riscos relacionados a atividade de tratamento de dados pessoais. É a partir desse diagnóstico que "controles jurídicos, processuais e de segurança da informação podem ser aplicados"[24], o que favorece uma segura adequação a Lei Geral de Proteção de Dados, e possibilita a empresa a visão da real dimensão dos dados da quais trata, possibilitando assim a geração de importantes documentos como o relatório de impacto de proteção de dados, de políticas de boas práticas de governança, de manuais controles de crises e de planos emergenciais para incidentes em caso de vazamento de dados.

---

23 VARELLA, Luísa. **Tratamento de dados: como fazer em *compliance* com a LGPD?** 17 de fev. de 2020. Disponível em: https://www.compugraf.com.br/tratamento-de-dados-como-fazer-em-compliance-com-a-lgpd/. Acesso em 06 de jul. de 2020.

24 READ TIME. **Canvas do Mapeamento de Dados Pessoais para a LGPD**. 04 de mar. de 2020. Disponível em: https://www.neotel.com.br/blog/2020/03/04/canvas-do-mapeamento-de-dados-pessoais-para-a-lgpd/. Acesso em 07 de jun. de 2020.

4.1. Como Elaborar Um Mapeamento

É notória a dificuldade das empresas em saber como dar início ao processo de mapeamento de dados. Fazer o mapeamento de fluxo dos dados pessoais exige um trabalho conjunto entre os múltiplos setores corporativos, o que envolve uma equipe técnica e jurídica altamente capacitada.

O primeiro passo na elaboração do mapeamento de dados é "a identificação do inventário, o desenho de fluxos e a associação aos sistemas". Em seguida tem se iniciada a interpretação desses dados com o fito de identificar eventuais falhas na proteção e segurança dessas informações, é também nesse momento que a empresa "designa para cada dado pessoal qual é a base legal para justificar o processamento daquela informação", o que possibilita a criação de um Diagnóstico de Riscos e Conformidade[25].

Nesse contexto, a LGPD pede que as empresas responsáveis pelo tratamento de dados pessoais se atentem a alguns parâmetros antes darem início ao processo de mapeamento de dados, são eles:

> Os objetivos do processamento de dados;
>
> As categorias de dados pessoais que estão sendo processadas;
>
> Detalhes de quaisquer transferências de dados para outros países;
>
> Por quanto tempo os dados serão mantidos;
>
> As medidas de segurança técnica e organizacional em vigor (criptografia, controles de acesso, etc.)[26].

25 PRICACY TOOLS. **Mapeamento de Dados: o seu inventário de informações**. 09 de out. de 2019. Disponível em: https://privacytools.com.br/mapeamento-de-dados-o-seu-inventario-de-informacoes/. Acesso em 07 de jul. de 2020.

26 CRUZ, Leandro Saad. **Mapeamento de dados para LGPD**. 17 de jun. de 2019. Disponível em: https://medium.com/@leandrosaad/mapeamento-de-dados-para-lgpd-c36413d54b73. Acesso em 11 de jun. de 2020.

Dando continuidade a esse procedimento, o manual de implementação da LGPD elaborado pela juíza e professora em direito digital, Viviane de Nóbrega Maldonado, elenca uma série de pontos essenciais que devem estar presentes no mapeamento de dados, são eles: a categoria de dados; o volume e o fluxo de dados; as etapas de gestão desses dados; as principais utilizadas no tratamento do fluxo de dados; os locais de onde os dados são coletados, armazenados e processados; a origem desses dados; as campanhas de *marketing* voltadas a informação do tipo e tratamento de dados; o modo de como são compartilhadas as informações pessoais com terceiros; a indicação das empresas cujos dados são compartilhados; a abrangência territorial onde a empresa exerce sua atividade; o modo de como se dá a transferência internacional de dados; a base legal a qual se submete a atividade empresarial direcionada a manipulação desses dados; se a política de privacidade interna está de acordo com os requisitos da LGPD; a identificação de dados pessoais pertencentes a menores de idade; a retenção e extinção de dados; a identificação dos principais mecanismos de controle de segurança; e por último se a gestão de dados pessoais da empresa possibilita o pleno gozo do exercício de seus direitos previstos pela legislação que regulamente a matéria de proteção de dados.[27]

Consoante o entendimento relatado, essa adequação pode ser um processo demorado, exige uma equipe técnica altamente qualificada e um certo grau de investimento financeiro, todavia o mapeamento de dados se torna fundamental, dado o advento da Lei Geral de Proteção de Dados e das novas transformações do mercado global.

CONSIDERAÇÕES FINAIS

Com o propósito de atender a necessidade de uma efetiva tutela no que tange a regulamentação do tratamento de dados pessoais no Brasil e

27 MALDONADO, Viviane de Nóbrega. **Lei Geral de Proteção de Dados pessoais: manual de implementação.** São Paulo: Thomson Reuters Brasil, 2019. p. 54-57.