Márcio Guimarães Konopczyk

Riscos, auditoria e resposta a incidentes

Senac

Dados Internacionais de Catalogação na Publicação (CIP)
(Simone M. P. Vieira - CRB 8ª/4771)

Konopczyk, Márcio Guimarães
Riscos, auditoria e resposta a incidentes / Márcio Guimarães Konopczyk. – São Paulo : Editora Senac São Paulo, 2022. (Série Universitária)

Bibliografia.
e-ISBN 978-85-396-3286-2 (ePub/2022)
e-ISBN 978-85-396-3287-9 (PDF/2022)

1. Informação – Sistemas de armazenagem e recuperação – Medidas de segurança 2. Gestão da segurança da informação : Gestão de riscos 3. Segurança da informação : Rede de computadores : Gestão de riscos 4. Plano de contingência 5. Lei Geral de Proteção de Dados Pessoais (LGPD) I. Título. II. Série.

22-1496t

CDD – 005.8
BISAC COM043050

Índice para catálogo sistemático
1. Gestão da segurança da informação : Gestão de riscos 005.8

RISCOS, AUDITORIA E RESPOSTA A INCIDENTES

Márcio Guimarães Konopczyk

Administração Regional do Senac no Estado de São Paulo

Presidente do Conselho Regional
Abram Szajman

Diretor do Departamento Regional
Luiz Francisco de A. Salgado

Superintendente Universitário e de Desenvolvimento
Luiz Carlos Dourado

Editora Senac São Paulo

Conselho Editorial
Luiz Francisco de A. Salgado
Luiz Carlos Dourado
Darcio Sayad Maia
Lucila Mara Sbrana Sciotti
Luís Américo Tousi Botelho

Gerente/Publisher
Luís Américo Tousi Botelho

Coordenação Editorial/Prospecção
Dolores Crisci Manzano
Ricardo Diana

Administrativo
grupoedsadministrativo@sp.senac.br

Comercial
comercial@editorasenacsp.com.br

Acompanhamento Pedagógico
Mônica Rodrigues dos Santos

Designer Educacional
Priscila Cristina do Nascimento

Revisão Técnica
Fabio Luiz Lettieri da Costa

Preparação e Revisão de Texto
AZ Design Arte e Cultura Ltda.

Projeto Gráfico
Alexandre Lemes da Silva
Emília Correa Abreu

Capa
Antonio Carlos De Angelis

Editoração Eletrônica
Sidney Foot Gomes

Ilustrações
Sidney Foot Gomes

Imagens
Adobe Stock Photos

E-book
Rodolfo Santana

Editora Senac São Paulo
Rua 24 de Maio, 208 – 3º andar
Centro – CEP 01041-000 – São Paulo – SP
Caixa Postal 1120 – CEP 01032-970 – São Paulo – SP
Tel. (11) 2187-4450 – Fax (11) 2187-4486
E-mail: editora@sp.senac.br
Home page: http://www.livrariasenac.com.br

Sumário

Capítulo 1

Privacidade de dados

O objetivo deste capítulo é despertar a plena consciência da importância da privacidade de dados pessoais, todos os seus princípios e suas políticas, permissões e exceções para o seu uso, o que é e o porquê da criação da LGPD (Lei Geral de Proteção de Dados), suas principais características e as semelhanças com a GDPR (General Data Protection Regulation) europeia, quem são os personagens que serão os responsáveis pelos dados e como os dados devem ser disponibilizados, bem como as possíveis consequências de um vazamento.

1 Lei Geral de Proteção de Dados (LGPD)

A LGPD, sigla para Lei Geral De Proteção de Dados Pessoais (Lei nº 13.709/2018), tem como objetivo principal disciplinar todos os procedimentos para armazenamento, coleta e manipulação de dados pessoais de pessoas naturais, que sejam identificadas ou identificáveis, em território brasileiro.

Segundo consta em seu artigo 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 (BRASIL, 2018).

Ela propõe uma significativa mudança no sistema de proteção de dados brasileiro. Estabelece normas específicas para coleta, uso, tratamento e armazenamento de dados pessoais e abrange todos os setores da economia, principalmente nas transações entre clientes, fornecedores, serviços de terceiros, funcionários e as relações comerciais nacionais e internacionais, desde que sejam manipuladas em território brasileiro. A lei não especifica se o meio em que os dados estejam armazenados sejam somente digitais. Isso significa que os arquivos com documentos pessoais em espécie também estão sob a proteção da lei.

A LGPD foi criada a partir da GDPR (General Data Protection Regulation), que é a versão europeia desta lei. A LGPD foi criada no ano de 2012, regulamentada em 2016 e finalmente implantada em 2018.

1.1 Tipos de dados (classificação, análise, coleta e cuidados) e o conceito de dado pessoal

Antes mesmo de fazer qualquer análise sobre dados, temos que conceituá-los no tempo e no espaço. Dado é qualquer representação

quantificada de alguma coisa. Desde o início, as empresas manipulam seus dados, os quais, quando armazenados, necessitam de alguns cuidados quanto a classificação, análise, coleta e armazenamento para que possam gerar informações úteis.

A classificação, em função do grande volume de informações, faz-se necessária, pois não há como analisar um dado ou uma informação colocada aleatoriamente para análise ou para segurança dos dados, visto que informações classificadas como confidenciais são passíveis de maior segurança do que outras informações que não necessitam de proteção.

A norma ISO 27001 exige que todas as informações sejam armazenadas, protegidas, que tenham sentido e também sejam devidamente classificadas de acordo com seu valor, criticidade, sensibilidade e requisitos legais. Elas também são identificadas como confidencial, restrita, para uso interno ou pública.

Quanto à análise, os dados, quando armazenados e classificados corretamente de acordo com sua importância, oferecem um poderoso conjunto de informações para que, ao serem compilados, possam facilitar a tomada de decisões mais adequadas nos mais diversos tipos de negócios.

Em relação à coleta de dados, é uma atividade que tem como objetivo captar a informação através de uma ferramenta específica de coleta. Ela ocorre quando há a necessidade específica para cumprimento legal (emissão de nota fiscal, cupom fiscal etc.), para uso estatístico em campanhas de marketing ou para atividades de um site que exige interação com seus usuários.

Mas para que todo armazenamento de dados faça sentido, há a necessidade premente da tomada de cuidados para sua segurança. Os dados armazenados passam a fazer parte do ativo da empresa que detém as informações, e todos os cuidados em seu armazenamento devem ser tomados para que não haja perda ou, o que é pior, vazamento indevido.

1.2 Princípios da proteção de dados pessoais e a privacidade dos dados

Para o armazenamento e coleta de dados, os responsáveis deverão seguir alguns princípios para a sua proteção, conforme determina a lei. Esta proteção deverá seguir alguns critérios importantes, que fazem parte do artigo 6º da LGPD e estão destacados a seguir:

1. Finalidade: realização de tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
2. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
3. Necessidade: limitação do tratamento ao mínimo necessário para realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
4. Livre acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
5. Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
6. Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
7. Segurança: utilização de medidas 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 difusão.

8. Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

9. Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

10. Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A privacidade de dados é um segmento da área de segurança da informação que normatiza como os dados são coletados, compartilhados e usados de maneira correta.

Para garantir esta privacidade, os funcionários que manipulam estas informações devem ser devidamente treinados em segurança e privacidade para que entendam como funcionam as rotinas e os processos de coleta, compartilhamento e uso de dados, principalmente os de caráter confidencial, e também preservar os direitos fundamentais dos titulares dos dados, que são:

- Consentimento explícito e inequívoco de uso.
- Saber até quando os dados serão manuseados.
- O direito de solicitar e verificar seus dados de forma fácil e gratuita.
- O direito de excluir seus dados quando assim o desejarem.

1.3 Permissões e exceções para o uso de dados

A LGPD possui alguns princípios básicos que regem as permissões e exceções para o uso de dados. As permissões que constam na LGPD têm como objetivo regulamentar os seguintes aspectos:

- O titular deverá fornecer uma autorização por escrito e com assinatura para que seus dados pessoais sejam coletados e o

controlador deverá, neste consentimento, esclarecer de maneira inequívoca a finalidade da coleta e o tratamento que será realizado, o prazo legal que as informações permanecerão de posse do controlador e quando serão descartadas ou anonimizadas.

- Em seu artigo 5º, inciso X, a LGPD descreve que o tratamento de dados pode ocorrer na forma de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, alteração, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração e eliminação de dados. E para que todas estas ações sejam realizadas, o titular dos dados pessoais deverá consentir por escrito sua autorização.

Como exemplos de finalidades para uso de dados coletados podemos citar: administrar folhas de pagamentos, envio de promoções via e-mail, publicar uma foto ou deletar documentos em uma rede social, gravações em vídeo do movimento nos corredores de um shopping, quando uma empresa armazena os endereços IP de seus clientes etc.

Em relação às exceções, a LGPD em seu artigo 4º diz que é permitido tratar dados sem consentimento do indivíduo nos seguintes casos:

a. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos.

b. Executar política pública prevista em lei.

c. Realizar estudos através de órgãos de pesquisa.

d. Prevenir fraudes contra o titular.

e. Cumprir uma obrigação legal.

f. Tutelar ações feitas por profissionais das áreas da saúde ou sanitária.

g. Defender direitos em processos.

h. Proteger o crédito.

i. Executar contratos.

j. Preservar a vida e a integridade física de uma pessoa.

k. Atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

l. Realizado para fins exclusivamente jornalísticos e artísticos ou ainda acadêmicos, porém, nesta hipótese deverá seguir as normas de consentimento previstas nos artigos 7º e 11º da LGPD.

1.4 Políticas de privacidade de dados

O assunto é regulamentado, no Brasil, principalmente pela Lei Geral de Proteção de Dados Pessoais (LGPD), lei que estabeleceu uma série de exigências àqueles que realizam operações de tratamento de dados pessoais.

Uma política de privacidade de um site ou de um aplicativo é um conjunto de termos e informações que descrevem todas as práticas realizadas em relação às informações de visitantes ou usuários coletadas por um site ou aplicativo.

A função da política de privacidade é esclarecer para o usuário como esses dados serão utilizados e para qual finalidade. Há inúmeras formas de coleta de dados pessoais, dos quais destacamos:

a. Dados de contato enviados pelo próprio usuário.

b. Informações de comportamento do usuário no site ou aplicativo.

c. Informações de navegação.

d. Localização.

e. Comportamentos e preferências diversas.

f. Informações sobre as páginas que são visitadas pelo usuário.

Além de todas estas formas de coleta, é importante esclarecer para quem está acessando a página ou o aplicativo que estas informações poderão ser repassadas para terceiros. Na medida do possível, deve-se informar quem são esses terceiros e por que estas informações estão sendo repassadas para que o usuário possa escolher se quer ou não liberar seus dados para isso.

1.5 LGPD – estrutura, princípios, responsabilidades e polêmicas

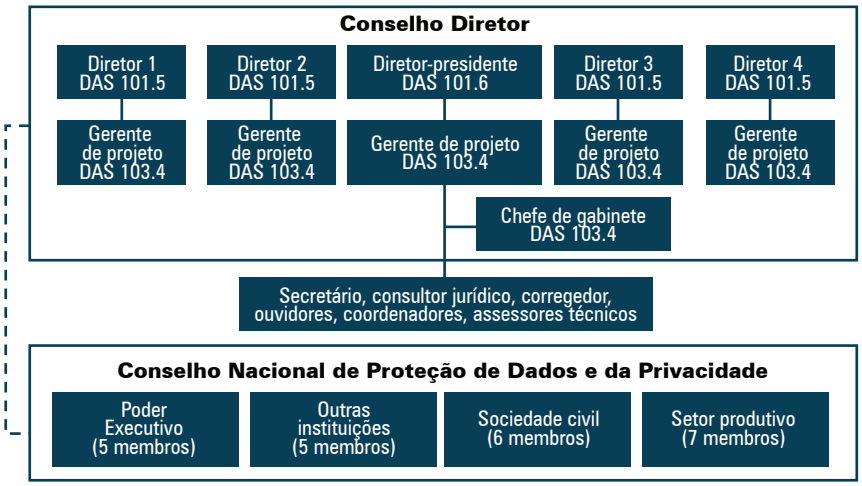
Segundo consta no Tribunal de Justiça do Estado de São Paulo, a Lei nº 13.709/2018 dispõe sobre o tratamento de dados pessoais, nos meios físicos e digitais, inclusive por pessoa jurídica de direito público, com o objetivo de proteger os direitos fundamentais da liberdade e de privacidade e o livre desenvolvimento da personalidade natural. As normas gerais contidas na lei são de interesse nacional e devem ser observadas pela união, estados, Distrito Federal e municípios.

1.5.1 Estrutura

Para cumprimento das normas da LGPD foi criado um órgão de controle, a Agência Nacional de Proteção de Dados (ANPD), cuja estrutura está representada na figura 1 a seguir.

A ANPD tem 36 cargos, sendo 16 em comissão remanejados (servidores contratados pela livre escolha e que já atuam em órgãos ligados à ANPD que serão remanejados nos novos cargos) e 20 funções comissionadas do Poder Executivo. Entre outras tarefas, a agência vai fiscalizar o cumprimento da lei, elaborar as diretrizes do Plano Nacional de Proteção de Dados e aplicar as sanções administrativas nas empresas que não cumprirem a LGPD.

Figura 1 – Estrutura organizacional da ANPD



Fonte: adaptado de BRASIL (2021).

PARA SABER MAIS

Para conhecer a estrutura da ANPD na íntegra, consulte sua página na internet.

1.5.2 Princípios da LGPD

Os princípios da LGPD abordam os seguintes assuntos:

a. Finalidade: os dados pessoais não poderão ser coletados com finalidades genéricas ou indeterminadas. O tratamento deverá ter fins específicos, legítimos, explícitos e informados, além de esclarecer para que fim a informação será usada.

b. Adequação: os dados coletados do titular devem ter compatibilidade com a finalidade apresentada; isto é, a informação que

está sendo coletada deve ser de acordo com a apresentada no consentimento.

c. Necessidade: por ocasião da coleta, as informações devem estar de acordo com a necessidade para atingir a finalidade.

d. Livre acesso: o titular dos dados tem o direito de consultar a qualquer momento, de forma simples e gratuita, todos os dados que a empresa armazenou a seu respeito, inclusive informando o que está sendo feito com os dados e o prazo limite que as informações serão descartadas.

e. Qualidade dos dados: o titular dos dados deve ter a garantia de que a empresa irá preservar os dados de forma verdadeira e atualizada, além da necessidade de que os dados sejam exatos e relevantes e estejam de acordo com a finalidade de seu tratamento.

f. Transparência: as informações que forem tratadas pela empresa em todos os meios de comunicação deverão ser claras, precisas e verdadeiras. O compartilhamento de qualquer informação com terceiros deverá ter o consentimento do titular.

g. Segurança: é de total responsabilidade da empresa a garantia de proteção dos dados pessoais acessados por terceiros. Mesmo que sejam autorizados, os dados deverão ser protegidos nos casos de invasão não autorizada, acidentes de qualquer natureza que venham a comprometer a integridade das informações ou ainda a difusão dos dados da base de armazenamento.

h. Prevenção: é de vital importância que as empresas adotem medidas preventivas para que não ocorram danos nos dados dos titulares.

i. Não discriminação: os dados pessoais jamais poderão ser usados para discriminar ou promover abusos ou qualquer forma de discriminação.

j. Responsabilização e prestação de contas: além de cumprir integralmente a lei, as empresas devem ter provas e evidências de todas as medidas adotadas para demonstrarem a sua boa-fé e a sua diligência.

Como responsabilidades, temos que:

k. O artigo 42 da LGPD determina que

> 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, será obrigado a repará-lo (BRASIL, 2018).

A LGPD traz, ainda, previsão expressa de responsabilidade solidária dos operadores e controladores. Nesse sentido, conforme disposição do inciso I do § 1º do artigo 42,

> o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador [...] (BRASIL, 2018).

Já os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, conforme inciso II do § 1º do artigo 42 da LGPD, respondem solidariamente (BRASIL, 2018).

1.6 Disponibilização de dados

A LGPD estabelece que a disponibilização de dados deverá ser apenas para as finalidades específicas para as quais foram coletadas e desde que devidamente informadas aos titulares. O consentimento do titular deve ser inequívoco, fornecido por escrito ou por outro meio que demonstre a manifestação de vontade. É importante lembrar que os

dados disponíveis, autorizados pelo titular, não são somente os armazenados em formato digital e sim todos, mesmo aqueles coletados no formato tradicional, isto é, as fichas de informações pessoais em papel.

1.7 Vazamento de dados

Mas afinal, o que é vazamento de dados?

Ele ocorre quando os dados pessoais de uma determinada instituição são extraídos de maneira criminosa por uma pessoa (hacker) ou uma instituição que não tem o mínimo de responsabilidade em suas ações, com o objetivo de vender esses dados na 'deep web', o 'submundo' da internet.

O Brasil está entre os países que mais sofrem os famosos ciberataques, e esses vazamentos demonstram claramente que nossa estrutura de proteção e monitoramento deste crime estão longe de possuir um controle rigoroso e punitivo.

Em janeiro de 2021 houve um vazamento de dados pessoais e sensíveis de 223 milhões de brasileiros. Entre as informações que foram expostas neste vazamento estavam número do CPF, nome completo, data de nascimento, entre outras informações de caráter sensível, como o valor da fatura do cartão de crédito (CORACCINI, 2021).

Embora a empresa que sofreu o vazamento não seja culpada pelo ocorrido, por se tratar de um crime cometido por terceiros, sua responsabilidade sobre o vazamento é total, e todas as consequências decorrentes deste vazamento são do controlador, isto é, da empresa que tinha os dados armazenados.

1.8 Agentes de tratamento de dados na LGPD: controlador, operador, encarregado

A LGPD em seu artigo 5º, incisos V, VI, VII e VIII, prevê em seu texto alguns personagens (BRASIL, 2018):

V. titular: pessoa natural a que se referem os dados pessoais que são objeto de tratamento.

VI. controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

VII. operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

VIII. encarregado: 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). Este profissional foi criado a partir da lei europeia GDPR e é denominado Data Protection Officer ou, simplesmente DPO.

PARA SABER MAIS

Para aprofundar seus conhecimentos acerca da LGPD, consulte o livro *Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação*, de Lara Rocha Garcia et al. (2020).

2 GDPR – General Data Protection Regulation

O GDPR é um regulamento do Parlamento Europeu e Conselho da União Europeia que estabelece regras sobre a privacidade e proteção de dados de cidadãos da União Europeia e Espaço Econômico Europeu.

A sigla significa General Data Protection Regulation ('Regulamento Geral sobre a Proteção de Dados'). Ela revoga a lei Data Protection Directive (DPD), de 1995, que foi o primeiro passo europeu para a proteção de dados.

Este regulamento teve início em janeiro de 2012 e apenas em dezembro de 2015 seu texto final foi concluído, mas somente em maio de 2018 é que sua vigência passou a vigorar.

A globalização da internet, a hiperconectividade e as milhares de inovações tecnológicas levaram à obtenção e ao uso de dados de usuários a um nível bem mais intenso, ocasionando uma série de problemas de ordem ética em relação aos quais os poderes governamentais nunca demonstraram qualquer tipo de preocupação.

2.1 Fundamentos da GDPR

A GDPR, em seu artigo 1º, apresenta seus fundamentos, dos quais destacamos os principais:

1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

2. Ele defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que concerne ao tratamento de dados pessoais (GPDR, 2021, tradução nossa).

2.2 Principais diferenças entre LGPD e GDPR

A GDPR, por ser mais antiga e desde 1995 ter iniciado alguns ensaios sobre o assunto, sem dúvida alguma possui um respaldo legal mais robusto do que a LGPD.

Apesar de abordarem o mesmo assunto, que é a proteção de dados pessoais e privacidade, a LGPD e a GDPR possuem algumas diferenças marcantes que se referem diretamente a normas específicas prévias à LGPD e à GDPR, as quais apontamos a seguir.

2.2.1 Sobre técnicas de segurança

Aqui no Brasil não existem regras próprias que determinam como as técnicas de segurança devem ser feitas, e as empresas precisam resolver estas questões por meios próprios. A orientação sobre as técnicas de segurança sobre os dados pessoais são determinadas pela ANPD.

A GDPR é mais específica neste assunto ao exigir medidas para manter os bancos de dados pessoais mais seguros e determina que os dados sejam encriptados ou pseudoanonimizados.

2.2.2 Sobre marketing direto

As informações coletadas na comercialização direta referem-se ao tratamento de dados pessoais para fins de criação de perfil de consumo e marketing e para, consequentemente, poder oferecer produtos ou serviços mais adequados ao perfil dos consumidores.

Na GDPR existem normas específicas que permitem a coleta de dados para este fim. Os titulares dos dados podem, a qualquer momento, se opor ao processamento de seus dados para estas finalidades.

A LGPD não aborda este assunto de forma direta, mas por ocasião da coleta de dados, deverá ser feita com autorização clara e inequívoca do

titular e não implícita, mesmo quando o tratamento siga as regras gerais de objeção, segurança e consentimento dos titulares dos dados pessoais.

2.2.3 Sobre dados sensíveis

A LGPD em seu artigo 5º, inciso II, considera que dado sensível é:

> Qualquer 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 (BRASIL, 2018).

Na LGPD, os dados sensíveis só podem ser tratados nas hipóteses previstas em lei. O tratamento, independentemente do consentimento do titular, pode ocorrer em duas exceções.

PARA SABER MAIS

Para conhecer essas exceções e a LGPD na íntegra, faça a leitura completa da lei (BRASIL, 2018).

Quanto aos dados sensíveis, autônomos, empresas e governo também podem tratá-los se tiverem o consentimento explícito da pessoa e para um fim definido. Sem consentimento do titular, a LGPD define que isso é possível quando for indispensável em situações ligadas a: uma obrigação legal; políticas públicas; estudos via órgão de pesquisa; um direito, em contrato ou processo; preservação da vida e da integridade física de uma pessoa; tutela de procedimentos feitos por profissionais das áreas da saúde ou sanitária; e prevenção de fraudes contra o titular.

A GDPR, em seu artigo 9, tem regras praticamente semelhantes às da LGPD, já que dados sensíveis são o objetivo principal das duas leis.

2.2.4 Sobre a relação entre controlador e operador

A LGPD determina que o controlador é o responsável pelas informações dos titulares e deve instruir o operador quanto a como o tratamento de dados deve ser realizado, de modo que esta relação é realizada de forma natural, sem a necessidade de cláusulas contratuais. Na GDPR, esta relação deve ser realizada contratualmente ou por meio de qualquer outro ato jurídico que vincule operador e controlador.

2.2.5 Sobre o relatório de impacto

Na LGPD, em seu artigo 5º, inciso XVII, este relatório é de total responsabilidade do controlador, mas não há regra específica sobre a obrigatoriedade de sua realização. Na GDPR, o relatório de impacto à proteção de dados pessoais deve ser elaborado quando o tratamento resultar em elevado risco ao direito e à liberdade das pessoas.

Considerações finais

Ao longo deste capítulo abordamos os assuntos mais importantes sobre privacidade de dados e também mais detalhadamente sobre tipos de dados, proteção, permissões, políticas e demais assuntos pertinentes. Abordamos sobre a LGPD, sobre a GDPR e suas principais diferenças.

Nosso intuito foi o de fazer com que você reflita sobre os tópicos apresentados, além de buscar fomentar a pesquisa complementar sobre os temas, provocar discussões, estimular o estudo mais aprofundado dos tópicos abordados nos subcapítulos e enriquecer o seu conhecimento.

Referências

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD): Estrutura. 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/estrutura-organizacional-1. Acesso em: 25 jun. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). **Diário Oficial**: seção 1, p. 59, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2021.

CORACCINI, Raphael. Fotos e até salários estão entre os dados vazados de 223 milhões de brasileiros. **CNN Brasil**, [s.l.], 27 jan. 2021. Disponível em: https://www.cnnbrasil.com.br/business/fotos-e-ate-salarios-estao-entre-os-dados-vazados-de-223-milhoes-de-brasileiros/. Acesso em: 25 jun. 2021.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: guia de implantação. São Paulo: Blucher, 2020.

GDPR. Regulamento Geral sobre Proteção de Dados. 2021. Disponível em: https://gdpr.eu/. Acesso em: 25 jun. 2021.