Noções essenciais da proteção de dados

Módulo 1

Análise e Ciência de Dados

EV.G
Uma iniciativa ENAP

Fundação Escola Nacional de Administração Pública

Diretoria de Desenvolvimento Profissional

Conteudista/s
Priscilla Regina da Silva (Conteudista, 2021).

Enap, 2021
Fundação Escola Nacional de Administração Pública
Diretoria de Desenvolvimento Profissional
SAIS - Área 2-A - 70610-900 — Brasília, DF

Sumário

Módulo

1 Noções essenciais da proteção de dados

Unidade 1. LGPD: O novo marco normativo do Brasil

Objetivo de Aprendizagem:
Explicar a importância da Lei Geral de Proteção de Dados na gestão das atividades do setor público.

1.1 A importância da LGPD

A **Lei 13.709/18** é a primeira lei brasileira dedicada especialmente à regulação do tratamento de dados pessoais em todo o território nacional. Trata-se de um grande marco normativo nacional.

É importante salientar, no entanto, que o Brasil se insere tardiamente no debate sobre o tema, já que a lei faz parte da quarta geração de leis de proteção de dados. Ou seja, outros países já pensam em regulação de proteção de dados há bons anos.

A primeira geração de leis sobre o tema data da década de 1970 e, sob o foco na esfera governamental, tinha a pretensão de regular a criação e o funcionamento de grandes bancos de dados, através da concessão de autorizações. Nesse contexto, já era possível falar no surgimento dos princípios da proteção e da precaução - estratégias jurídicas que podem ser aplicadas tanto às situações de risco quanto de perigo, visando a impedir o risco de perigo abstrato.

SAIBA MAIS

A classificação evolutiva dessas leis é realizada por Viktor Mayer-Schonberger. Cf.: MAYER-SCHONBERER, Viktor apud MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Sairava, 2014. p. 37.

Exemplo de leis de primeira geração:

1. Lei do de Hesse de 1970;
2. Lei Nacional de Proteção de Dados da Suécia de 1973 - *Data Legen Privacy Act* dos Estados Unidos de 1974.

Com a proliferação de centros de processamento de dados, essas leis logo se mostraram obsoletas. O final da década de 1970 foi, assim, marcado pela segunda geração de leis sobre proteção de dados, que evoluíram para o consentimento do cidadão para o tratamento de dados com um propósito específico. O fluxo de informações pessoais passa a não precisar mais ser autorizado pelo Estado, cabendo ao próprio indivíduo, por meio do consentimento, decidir pelo tratamento dos seus dados pessoais.

Exemplo de leis de segunda geração:

1. Lei Francesa de Proteção de Dados Pessoais de 1978 - *Informatique et Libertés*;
2. Lei Alemã de Proteção de Dados de 1978 - *Bundesdatenschutzgesetz*;
3. Lei austríaca de 1978 - *Datenschutzgesetz*.

A **terceira geração** de normas de proteção de dados pessoais tem como marco a decisão do Tribunal Constitucional alemão no julgamento sobre a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 1983", espécie de Lei do Censo. O texto legal foi impugnado por diversos grupos de cidadãos que vislumbravam os riscos sobre a coleta ampla de dados pessoais. O caso chegou à Corte Constitucional alemã, que decidiu pela inconstitucionalidade parcial da lei, defendendo a existência de um direito à "autodeterminação informativa". Através da decisão do Tribunal Constitucional, o tratamento não transparente de dados pessoais foi repudiado a partir da ideia da dignidade da pessoa humana e do livre desenvolvimento da personalidade.

O direito à autodeterminação informativa é compreendido como forma de garantir o controle do cidadão sobre suas próprias informações a partir de uma série de direitos. Ou seja, ele certifica que o titular tenha domínio sobre os seus dados pessoais, ainda que o tratamento dessas informações seja legítimo.

Exemplo de Norma de Terceira Geração:

1. Decisão do Tribunal Constitucional Alemão sobre a Lei do Censo, 1983.

A **quarta geração** das leis de proteção de dados veio para superar as deficiências dos períodos anteriores, tendo como escopo principal o fortalecimento da posição do indivíduo no controle de seus dados pessoais; e, paradoxalmente, a retirada de certos assuntos da esfera do controle do indivíduo, em razão de sua acentuada relevância.

Exemplo de lei de Quarta Geração:

1. Diretiva 46/95 da União Europeia - Atualmente ***General Data Protection Regulation*** (Lei Geral de Proteção de Dados da União Europeia, ou GDPR).

A Lei Geral de Proteção de Dados Pessoais brasileira veio, desta forma, alinhada ao panorama internacional, introduzindo o Brasil no debate sobre o tema, potencialmente facilitando transações internacionais de dados e aproximando o Brasil do possível ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Antes que se falasse em uma Lei Geral de Proteção de Dados pessoais, o Poder Judiciário brasileiro aplicava outras leis para tratamento do tema no Brasil. Era comum a invocação do direito à privacidade como elemento primário à proteção de dados pessoais. Assim, aplicavam-se a Constituição Federal de 1988 (Art. 5º, X), Código Civil de 2002 (Art. 21), o Código de Defesa do Consumidor - aplicável aos casos relacionados ao consumo - o Marco Civil da Internet de 2014 - que prevê alguns direitos dos titulares posteriormente delimitados pela Lei Geral de Proteção de Dados.

SAIBA MAIS

Dentre os preceitos fundamentais do Marco Civil da Internet estão: a inviolabilidade da intimidade e da vida privada (Art. 7º, I); a proteção contra o fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do titular (Art. 7º, VII); o direito a informações claras e completas sobre o tratamento de dados pessoais (Art. 7º, VIII); e a necessidade de consentimento expresso e destacado sobre o tratamento de dados (Art. 7º, XI).

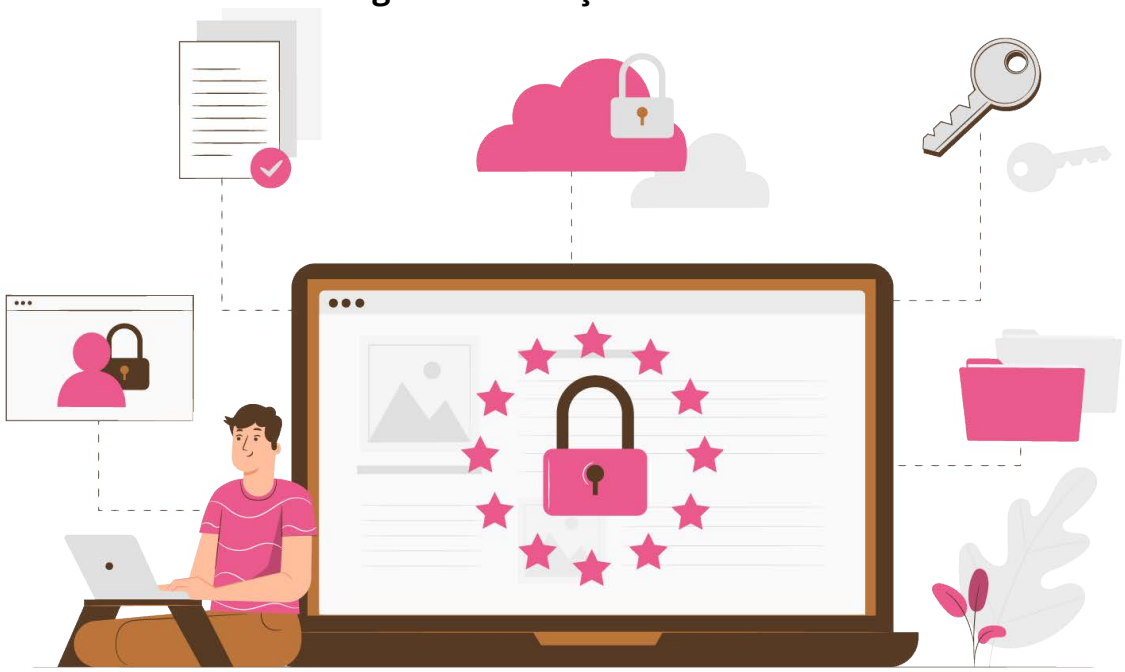
Outra importante lei sobre o tratamento de dados, desta vez para o setor público, é a Lei nº 12.527/2011. A Lei de acesso à Informação (LAI) regulamenta o direito constitucional de acesso às informações públicas, tendo criado “mecanismos que possibilitam, a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades”.

Ainda que as mencionadas leis tenham introduzido o tema no direito brasileiro, não se configuram suficientes para regular o tratamento de dados pessoais de modo geral.

Desta forma, buscando sanar as dificuldades sobre tratamento de dados em qualquer situação e tutelar os indivíduos em face da utilização cada vez mais ampla dos dados pessoais, compreendeu-se pela necessidade de uma lei mais específica para regular o tema e, assim, introduzir no Brasil uma cultura de proteção de dados. Assim, no dia 14 de agosto de 2018 foi sancionada e publicada a Lei nº 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Essa lei “inaugura no Brasil um regime geral de proteção de dados pessoais”.

Inspirada no Regulamento Geral de Proteção de Dados da União Europeia, a LGPD altera o Marco Civil da Internet e dispõe sobre o tratamento de dados pessoais, nos meios físicos ou meios digitais, por pessoa natural ou jurídica, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade natural, conforme seu art. 1º.

Figura 1. Proteção de dados.



Fonte: Freepik.

A LGPD tem aplicação a qualquer pessoa, seja natural ou jurídica de direito público ou privado que realize o tratamento de dados pessoais, online e/ou offline. Assim, podemos inferir que a Lei possui aplicação ampla e abrangente, abarcando além do setor privado, todos os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário, e Ministério Público, além das autarquias, fundações e empresas públicas, sociedades de economia mista e demais entidades controladas direta e indiretamente pela União, estados, Distrito Federal e municípios.

Laura Schertel Mendes e Danilo Doneda afirmam ser possível "identificar cinco eixos principais da LGPD em torno dos quais a proteção do titular dos dados se articula", assim definidos: "i) unidade e generalidade da aplicação da Lei; ii) legitimação para o tratamento de dados (hipóteses autorizativas); iii) princípios e direitos do titular; iv) obrigações dos agentes de tratamento de dados); v) responsabilização dos agentes". Estes pontos serão devidamente abordados ao longo do curso.

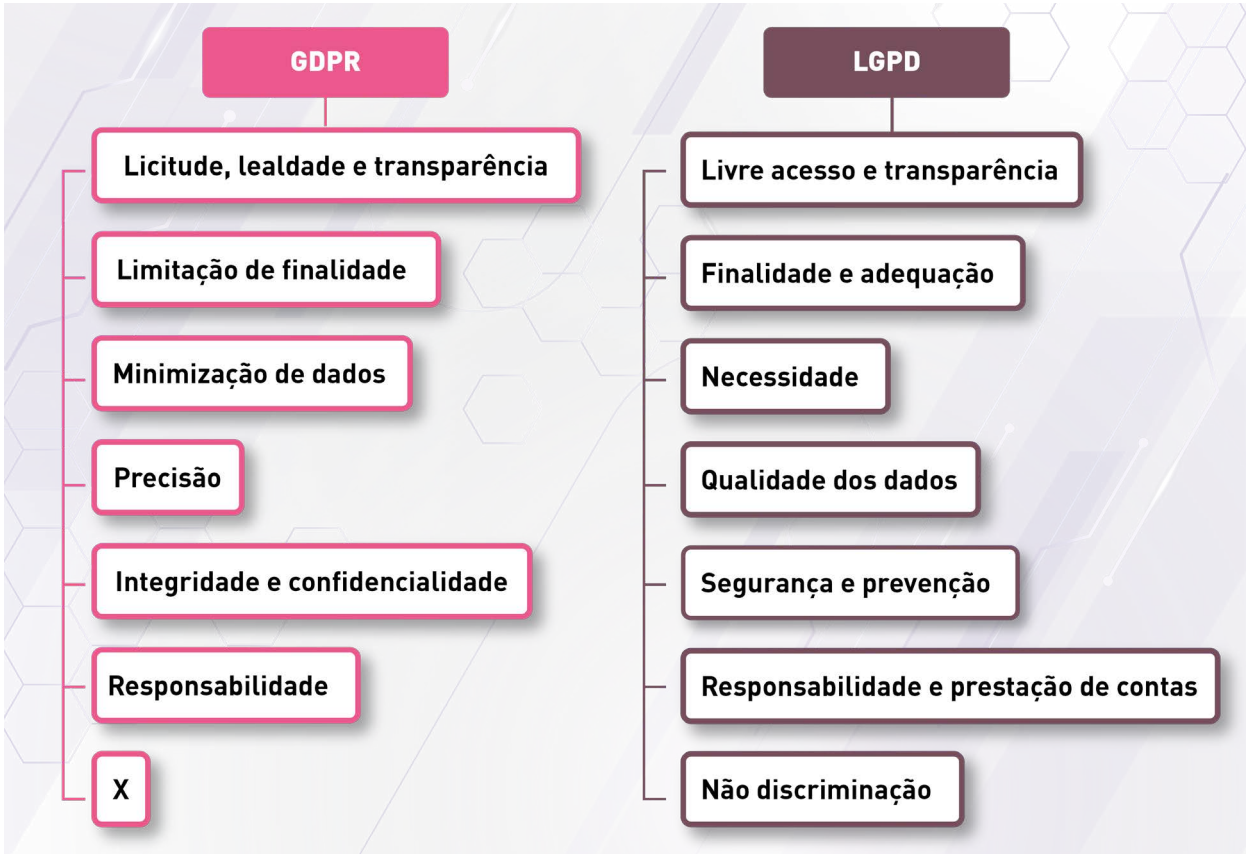
1.2 Princípios da LGPD e princípios da Administração Pública

Conforme vimos no tópico anterior, a Lei Geral de Proteção de Dados foi inspirada no Regulamento Europeu (GDPR). Da mesma forma que o GDPR, a LGPD elenca, no art. 6º da lei princípios que deverão nortear o tratamento de dados pessoais e a aplicação da legislação.

Os princípios norteadores nada mais são que ordens aos agentes de tratamento. Estes princípios devem ser observados como exigência mínima para uma boa atividade de tratamento de dados pessoais.

Antes de adentrarmos em cada um dos princípios da LGPD, vemos abaixo a listagem, de um lado, dos princípios elencados no GDPR, e do lado direito, os princípios elencados pela LGPD, em ordem de correspondência.

Figura 2. Princípios Gerais da Proteção de Dados.



Fonte: elaborado pela autora.

No caso do setor público, se já não fossem suficientes os princípios previstos no art. 37 da Constituição Federal de 1988 - São eles: legalidade, impessoalidade, moralidade, publicidade e eficiência -, os entes públicos também devem zelar pelo cumprimento dos princípios expostos no art. 6º da LGPD. Com isso, temos uma excelente combinação de princípios que, sendo respeitados, darão maior garantia da proteção de dados pessoais. Vamos a cada um deles.

Princípio da finalidade

De acordo com a LGPD não é possível tratar dados pessoais com finalidade genérica ou indeterminada.

O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Por propósitos legítimos, refere-se a uma finalidade movida pelo bom senso, legalidade, bons costumes e boa fé. Por propósitos específicos, compreende-se a ênfase em um objetivo determinado relevante para o ser. Por propósitos explícitos procura enfatizar o aspecto unívoco do tratamento, ou seja, não admitindo a equivocidade ou ambiguidade. Assim, o objetivo deve ser claro e previamente delineado, não permitindo que dúvidas possam surgir após ser especificado seu conteúdo.

A finalidade não poderá ser modificada durante o tratamento de dados pessoais.

Princípios da Administração Pública equivalentes: O princípio da finalidade se aproxima dos princípios da legalidade e da moralidade.

Princípio da Adequação

Os dados pessoais tratados devem ser compatíveis com a finalidade do serviço prestado, de acordo com o contexto do tratamento. Ou seja, para cada atividade-fim, prestação de serviço, deverá ser assinalada uma finalidade específica.

O princípio da adequação determina a relação entre a) o tratamento e a finalidade objetivada; b) o tratamento e a comunicação transmitida ao titular; c) a finalidade almejada e a comunicação transmitida ao titular; e, d) entre os três elementos, integradamente considerados.

Princípios da Administração Pública equivalentes: princípios da legalidade e eficiência.

Princípio da Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades. Associado à ideia de que, em um tratamento de dados pessoais, somente deve ser coletada a quantidade mínima de dados para se concretizar a atividade.

Os dados coletados devem ser pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

A aferição da necessidade pode ser transportada para situação em que a Administração Pública interfere no exercício da liberdade e da propriedade dos indivíduos, ora promovendo desapropriações, ora apreendendo alimentos deteriorados, estabelecendo condições para o exercício do comércio etc. Em todos os casos a intervenção, de acordo com o princípio da proporcionalidade, deverá dar-se por meio da adoção do ato administrativo mais suave à situação, constituindo-se, considerando a intensidade e extensão.

Princípio da Administração Pública equivalente: princípio da eficiência.

Princípio do 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.

Deve-se garantir, ainda, que antes da realização do tratamento, seja cientificado, o respectivo titular, da forma, gratuita, através da qual, possa acessar os dados tratados.

Princípio da Administração Pública equivalente: Princípio da publicidade

Princípio da 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.

Princípio da Administração Pública equivalente: Princípio da eficiência

Princípio da 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. O controlador de dados pessoais não poderá, assim, compartilhar dados dos titulares com outros agentes de forma oculta.

Ao exigir informações claras, a LGPD procura indicar que a utilização de conteúdo excessivamente técnico e até hermético não se compagina com o objetivo de tal princípio, que deve tornar as informações acessíveis ao público.

O conteúdo da transparência consuma-se, não só nos dados, antes e posteriormente tratados, como, também, dos agentes que tomaram parte do procedimento, ou seja, o controlador e o operador.

Princípio da Administração Pública equivalente: Princípio da publicidade

Princípio da 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.

Princípios da Administração Pública equivalentes: Princípios da impessoalidade e eficiência.

Princípio da Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Princípios da Administração Pública equivalentes: Princípios da impessoalidade e eficiência.

Princípio da Responsabilidade ou da Prevenção 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.

Princípios da Administração Pública equivalentes: Princípios da impessoalidade e eficiência.

Princípio da Não Discriminação

Não utilização de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

Princípios da Administração Pública equivalentes: Princípios da impessoalidade e eficiência.

Referências Bilbiográficas

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 210.

General Data Protection Regulation. Disponível em: https://gdpr-info.eu/. Acesso em 27/03/2022.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 27/03/2022.

MARIA, Isabela; PICOLO, Cinthya. **Autodeterminação Informativa:** Como esse Direito surgiu e como ele me afeta? Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em 27/03/2022.

MAYER-SCHONBERGER, Viktor apud MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 37.

Síntese Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em 27/03/2022

Unidade 2 - Características e conceitos

Objetivo de Aprendizagem:
Identificar características e conceitos sobre dados pessoais e dados pessoais sensíveis.

2.1 Dados pessoais e dados pessoais sensíveis

Existem quatro características de dados mencionadas ao longo da Lei Geral de Proteção de Dados: dados pessoais, dados pessoais sensíveis, dados anonimizados e dados pseudonimizados. Para cada tipo de dado, a LGPD estipula determinações próprias.

Figura 3. Características de dados mencionados ao longo da LGPD.

Fonte: elaborado pela autora.

Dados Pessoais

Dados pessoais são informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

Exemplos de dados pessoais:

- o nome e sobrenome;
- o endereço de uma residência;

- um e-mail que contenha nome e sobrenome nome.sobrenome@empresa.com;
- o número de identidade ou CPF;
- dados de localização (por exemplo, a função de dados de localização em um celular);
- um endereço IP (protocolo de internet);
- dados de conexão e navegação (cookies);
- os dados coletados por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca.

Exemplos de dados não considerados pessoais:

- o número de registo de empresa;
- email como info@empresa.com;
- dados anonimizados.

Dados pessoais sensíveis

Dentro do conjunto de dados pessoais, há ainda aqueles que exigem um pouco mais de atenção: são os sobre crianças e adolescentes; e os "sensíveis". São compreendidos como dados que potencialmente poderão ser utilizados para fins discriminatórios, em razão de revelarem pertencimento a determinado grupo social.

São considerados dados sensíveis:

- dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;
- filiação sindical;
- dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano;
- dados relacionados com a saúde;
- dados relativos à vida sexual ou orientação sexual da pessoa.

Cumpre salientar que a lista não é exaustiva, ou seja, é apenas exemplificativa. Além disso, é possível que dados que a princípio não configurem dados sensíveis por si só, quando potencialmente utilizados para fins de análise discriminatória, serão caracterizados como sensíveis. É o caso, por exemplo, de dados de localização serem utilizados para oferta de preços diferenciada sobre determinado serviço.

Nas palavras de Caitlin Mulholland (2018):

> **O princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou indução a resultados que seriam inequitativos. Esse princípio deve servir como base de sustentação da tutela dos dados sensíveis, especialmente quando estamos diante do exercício democrático e do acesso a direitos sociais, tais como o direito ao trabalho, à saúde e à moradia.**

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

Dados anonimizados

A LGPD define em seu art. 5º, inciso III, que dado anonimizado é aquele "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento". Define, ainda, no inciso XI, que a anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

O art. 12 define que os dados anonimizados não são considerados dados pessoais, salvo quando o processo de anonimização for reversível, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. O parágrafo 1º desse artigo tenta clarificar a definição de esforços razoáveis, colocando como parâmetros o custo e o tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis e utilização exclusiva de meios próprios. Já o parágrafo 3º estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre os padrões e técnicas de anonimização e realizar verificações sobre sua segurança, ouvido o Conselho Nacional de Proteção de Dados. Essa é uma

regulamentação que a ANPD deverá definir, a exemplo dos padrões técnicos mínimos de segurança para proteger os dados pessoais.

Dados pseudonimizados

A definição para dados pseudonimizados está no art. 13, parágrafo 4º. A pseudonimização é o "tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". Ou seja, o dado pseudonimizado tem um processo de reversão viável por meio de uso de informação adicional que o controlador mantém em ambiente separado, com controles de segurança.

Enquanto o dado anonimizado está fora do escopo de aplicação da LGPD justamente porque perde a característica de dado pessoal (não é possível associar um dado à pessoa), o dado pseudonimizado continua a seu regulado pela LGPD, tendo em vista justamente a possibilidade de associar o dado à pessoa a qual este dado se refere.

Casos ocorridos no Brasil denotam preocupação com relação à falta de critérios mínimos bem definidos para a anonimização de dados, de forma que a utilização de dados de geolocalização através das teles - dados estes, a princípio anonimizados - para a contenção da pandemia do novo coronavírus foram vazados.

Veja mais sobre em: DIAS, Tatiana. Vigiar e Lucrar. ***The Intercept Brasil***, 2020.

> **Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação da LGPD.**
>
> **A Lei Geral de Proteção de Dados dispõe que seja feita a anonimização sempre que possível, especialmente em casos de utilização para políticas públicas, tratamento de dados sensíveis e estudos por órgãos de pesquisa.**

Figura 4. Análise de dados.

Fonte: Freepik.

2.2 Requisitos para o tratamento de dados pessoais

A LGPD aplica-se a qualquer operação de **tratamento,** assim entendida como toda operação realizada com dados pessoais, como as que se referem a:

1. coleta;
2. acesso;
3. armazenamento;
4. arquivamento;
5. avaliação;
6. classificação;
7. comunicação;
8. controle;
9. difusão;
10. distribuição;
11. produção;
12. reprodução;
13. transferência;
14. utilização.

Estas operações de tratamento estarão presentes no ciclo de vida do dado pessoal da seguinte forma:

1. **coleta:** início do tratamento coleta e acesso;
2. **retenção:** armazenamento e arquivamento;
3. **processamento:** avaliação, classificação, comunicação e controle;
4. **compartilhamento:** difusão, distribuição, produção, reprodução e transferência;
5. **eliminação:** fim do tratamento.

Exemplo: coleta de dados pessoais para identificação de uma pessoa que elabora um pleito perante a administração. Nesse caso, a coleta de qualquer dado pessoal (nome, número de RG, etc.) está sujeita à aplicação da Lei.

No art. 7º LGPD elenca 10 requisitos para o tratamento de dados pessoais, também chamados de bases legais para o tratamento de dados. Cumpre mencionar que se trata de uma lista taxativa, ou seja, não cabe invocar outros requisitos para além daqueles mencionados em lei.

Os requisitos são os seguintes:

1) **Consentimento -** de acordo com o art. 5º, XII da LGPD, o consentimento coletado deverá ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

   Por livre, significa que o titular poderá escolher entre aceitar e recusar. Por informada e inequívoca, significa que não serão aceitas autorizações genéricas para o tratamento dos dados. O consentimento deverá ser para finalidades determinadas e não para "melhoria dos serviços" ou para "melhorar sua experiência".

   O consentimento será considerado nulo se tiver sido obtido com base em informações falsas, insuficientes ou que não tenham sido claras.

   As demais hipóteses configuram situações em que o consentimento não será solicitado.

2) **Cumprimento de obrigação legal ou regulatória pelo controlador** - ou seja, quando o controlador é obrigado a coletar seus dados por exigência do poder público (Receita Federal, por exemplo). É importante saber que, nesse caso, a dispensa do consentimento deve ser divulgada e a coleta de dados devidamente informada.

3) **Pela Administração Pública -** para a execução de políticas públicas previstas em leis e regulamentos. Por exemplo: campanhas de vacinação.

4) **Para a realização de estudos por órgãos de pesquisa** - nesse caso, a LGPD recomenda que sempre que possível o dado deve ser anonimizado, garantindo a privacidade dos titulares.

> **Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso à base de dados pessoais. A divulgação dos resultados em nenhuma hipótese poderá revelar dados pessoais. Não será permitida, em circunstância alguma, a transferência dos dados a terceiros.**

5) **Para a realização de contratos -** quando for necessário para a validação e execução de um contrato do qual o titular participe.

6) **Para processos judiciais ou administrativos -** é o caso da coleta e compartilhamento das informações para que o titular possa ingressar com uma ação judicial ou com um processo administrativo para requerer seus direitos (formalizar uma reclamação no Procon, por exemplo).

7) **Para a proteção da vida e para a tutela da saúde -** é o caso de um atendimento médico de emergência ou de qualquer outra situação na qual a vida e a integridade física estejam em risco.

   Dados referentes à sua saúde só poderão ser compartilhados nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses do titular.

8) **Quando necessário para atender aos interesses legítimos do Controlador** (somente dados pessoais estritamente necessários e para finalidades legítimas) - os legítimos interesses da empresa têm que ser comprovados em cada caso concreto, mediante comprovação da proporcionalidade e salvaguardas necessárias.

   Nota mental: o setor público não pode mais fazer uso do interesse legítimo como base legal. O legítimo interesse também não poderá ser invocado para justificar tratamento de dados sensíveis e dados de crianças e adolescentes.

9) **Para proteção do crédito -** é o caso do envio do nome de uma pessoa inadimplente para o cadastro do SPC ou da Serasa, por exemplo.

10) **Para os dados tornados manifestamente públicos pelo titular -** é o caso dos dados publicados pelo titular nas redes sociais, por exemplo.

IMPORTANTE

Mesmo para os casos em que não é pedido o consentimento, o tratamento de seus dados deve estar de acordo com a Lei.

Nota mental:

- **Não há no art. 7º nenhuma base legal hierarquicamente superior às demais.**
- **Trata-se de um rol taxativo**
- **Ainda que seja possível identificar mais de uma base legal para determinado tratamento de dados, é preciso indicar apenas uma, a mais adequada e segura para a situação concreta.**
- **Apesar de não haver hierarquia entre as possíveis bases legais, para facilitar uma análise concreta é recomendável analisar primeiro se o caso se enquadra nas situações mais objetivas (por exemplo, uma obrigação legal ou para a finalidade de políticas públicas pela administração pública) e, caso não seja possível enquadrar a atividade nessas situações, verifica-se a possibilidade de tratamento a partir de requisitos mais amplos, como o caso do legítimo interesse e do consentimento.**

VÍDEO

Requisitos para o tratamento de dados pessoais pelo setor público:
https://cdn.evg.gov.br/cursos/491_EVG/videos/modulo01_video01.mp4

2.3 Direitos dos Titulares

O titular deve ter acesso facilitado e de forma clara, adequada e visível às seguintes informações: finalidade específica do tratamento; forma e duração do tratamento; identificação e informações de contato do Controlador; informações sobre o uso compartilhado de dados pelo Controlador e a finalidade; responsabilidade dos agentes que realizarão o tratamento.

Qualquer alteração dessas informações deverá ser informada ao titular dos dados, que poderá anular o consentimento (quando a base legal para o tratamento for o consentimento) caso discorde das alterações. Se houver alteração da finalidade do tratamento, o titular tem o direito de ser informado previamente.

O titular também tem direito, de forma gratuita e através de requisição:

- À confirmação da existência do tratamento e o acesso aos dados.
- À correção de dados incompletos, inexatos ou desatualizados;

- Ao bloqueio ou à eliminação de dados desnecessários, excessivos ou em desacordo com a lei. Este direito poderá ser requisitado mesmo nos casos em que o consentimento não foi solicitado.
- À portabilidade dos dados a outro fornecedor de serviço ou produto. Ou seja, o titular tem o direito de requisitar a transferência dos dados para que a execução do serviço seja realizada por outro controlador. Este direito é limitado às capacidades técnicas disponíveis em razão da interoperabilidade dos sistemas e não inclui dados que já tenham sido anonimizados pelo Controlador.

  Veja mais sobre clicando aqui.
- À informação das entidades públicas e privadas com os quais o Controlador realizou uso compartilhado de dados.
- À anulação do consentimento a qualquer momento. O titular somente não poderá anular seu consentimento para tratamentos já realizados e para os quais tenha sido autorizada sua conservação (obrigação legal; pesquisa; uso próprio do Controlador, desde que anonimizados).

IMPORTANTE

Se houver vazamento dos dados, o titular tem o direito de ser comunicado imediatamente.

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: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (art. 16).

Referências Bibliográficas

MULHOLLAND, Caitlin. **Dados Pessoais Sensíveis e a tutela de Direitos Fundamentais**: Uma análise à Luz da Lei Geral de Proteção de Dados (Lei 13.709/18), 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603

DIAS, Tatiana. **Vigiar e Lucrar**. *The Intercept* Brasil, 2020. Disponível em: https://theintercept.com/2020/04/13/vivo-venda-localizacao-anonima/

SILVA, Priscilla. **Conheça a Biblioteca online de Portabilidade de Dados no Brasil.** Projeto portabilidade de dados. Disponível em: https://www.portabilidadededados.com.br/. Acesso em 27/03/2022.