b/luz

# DADOS DE SAÚDE E A LEI GERAL DE PROTEÇÃO DE DADOS

Estudo de Casos

# AUTORES:

/ Adriane Loureiro Novaes
/ Camila de Vito
/ Fernando Bousso
/ Gabriela Moribe
/ Luiza Balthazar
/ Matheus Botsman Kasputis
/ Odélio Porto Júnior
/ Rafael Pessoa
/ Renato Leite Monteiro

## Atualizado por:

/ Adriane Loureiro Novaes
/ Dandara Ramos Silvestre da Silva
/ Matheus Botsman Kasputis
/ Marina Almeida Costa Muçouçah

# Sumário



sumário clicável

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# Introdução:

A LGPD impacta significativamente o setor de saúde, especialmente em áreas como medicina de precisão e diagnóstica, e-Health e telemedicina. Entretanto, em vez de encarar a conformidade com LGPD como um ônus, as empresas podem explorar a legislação como uma oportunidade de gerar valor dentro das empresas, seja de reputação, melhoria de processos ou de inteligência de mercado.

Neste trabalho, buscamos trazer uma abordagem teórica e prática sobre a influência da LGPD no setor de saúde. Utilizando estudos de casos hipotéticos, exploramos as possíveis aplicações práticas da legislação, destacando desafios e oportunidades para as organizações.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

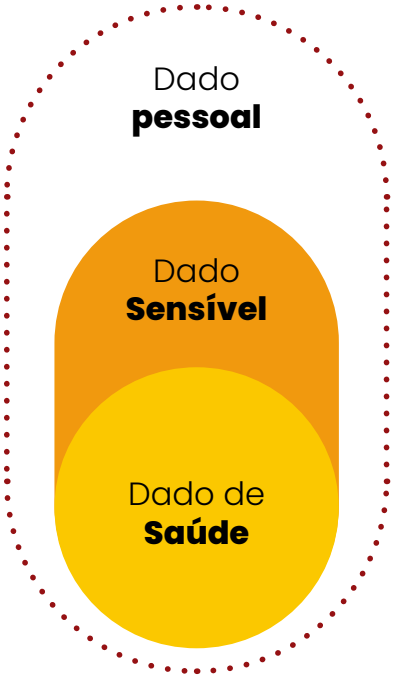
9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 1. Dado pessoal, dado sensível e dado de saúde:

*como legitimar o tratamento desses dados?*




**Caso:** uma determinada empresa X desenvolveu um aplicativo para atletas profissionais de alta performance terem resultados cada vez melhores. Para tanto, a Empresa trata dados pessoais do usuário, tais como peso, altura, marcador de passos diários, frequência de batimentos cardíacos, distâncias percorridas durante a prática da atividade física, duração da atividade física, entre outros dados. Sabendo da sanção da LGPD, a Empresa quer saber sobre quais dados a LGPD se aplica, bem como as bases legais que podem ser utilizadas para justificar o seu tratamento.

O caso hipotético apresentado acima envolve os conceitos de **(i) dado pessoal, (ii) dado sensível, (iii) dado de saúde e (iv) base legal** para o tratamento de dados pessoais. Abaixo, explicamos esses conceitos, para então aplicá-los na solução do caso.

De acordo com a LGPD, estes conceitos podem ser definidos da seguinte maneira:

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

## "Dado pessoal[1]":

é a informação relacionada a pessoa natural identificada ou identificável. Por exemplo, incluem-se nessa categoria nome, número de telefone, e-mail, entre outros, assim como identificadores únicos eletrônicos, como IP, cookies, beacons etc. Esse conceito também abrange dados que, isoladamente ou em conjunto, em um determinado contexto, possam permitir a identificação de alguém. Além disso, engloba dados que possam sujeitar uma pessoa natural individualizada a uma determinada atividade, comportamento ou ação (prática conhecida como *"singling out"*), às vezes tornando desnecessário saber efetivamente quem essa pessoa é (saber se trata de Maria ou João), desde que haja um identificar único atrelado a este indivíduo.

## "Dado sensível[2]":

é um conceito mais específico dentro da categoria de dado pessoal. Refere-se aos dados que, devido à sua sensibilidade, podem ser utilizados para fins discriminatórios ou para se tornarem identificadores únicos universais, exigindo, portanto, padrões mais rigorosos para seu tratamento. Incluem-se nesse grupo: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Esse conceito também abrange dados pessoais que, à primeira vista, podem não parecer sensíveis, como a localização de um indivíduo (p. ex. informações de geolocalização de uma pessoa que frequenta semanalmente uma determinada igreja ou espaço de culto) mas que, devido ao contexto de sua coleta, podem permitir inferir dados sensíveis – como a sua convicção religiosa[3].

[1] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso I.

[2] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso II.

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, §1º.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

## “Dado de saúde[4]”:

conforme exposto acima, os dados de saúde estão dentro da categoria de dados sensíveis. Esse conceito abrange, também, dados pessoais que, à primeira vista, podem não parecer ser de saúde, mas que, dentro de um contexto, podem permitir inferir dados sensíveis de saúde, como a frequência de corridas e batimentos cardíacos de um determinado indivíduo.

[4]BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso II.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

## "Base legal[5]":

para tratar dados pessoais é necessário que o agente de tratamento se fundamente em uma base legal. Bases legais são, portanto, as hipóteses que permitem o tratamento desses dados, dependendo da natureza do dado e a finalidade do tratamento. Cumpre salientar que as bases legais são distintas dependendo da natureza do dado. A LGPD traz 10 hipóteses para o tratamento dos dados pessoais[6] e 8 hipóteses para o tratamento de dados pessoais sensíveis[7], como os dados de saúde.

O legislador optou por conferir às bases legais o mesmo peso, isto é, o consentimento vale tanto quanto a base legal da tutela da saúde ou do legítimo interesse, sendo necessário verificar qual a base legal mais adequada para o contexto do tratamento, principalmente levando em consideração a finalidade almejada e a carga de participação do indivíduo no tratamento.

[5] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigos 7 e 11.
[6] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º. Incisos I a X.
[7] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11. Incisos I e II.

Já para os dados sensíveis, o legislador optou por privilegiar o uso da base legal do consentimento para tratamento de dados pessoais sensíveis, sendo as outras bases capazes de fundamentar um tratamento em caráter excepcional, somente para os casos em que a coleta dos dados for indispensável[8] para atingir o objetivo da base legal em comento.

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

Enumeramos as bases legais no quadro abaixo:

| **Dado pessoal** *(hipótese geral)* | **Dado sensível** *(hipótese específica)* |
|---|---|
| 1. consentimento;<br>2. obrigação legal;<br>3. políticas públicas;<br>4. estudos por órgão de pesquisa;<br>5. xecução de contrato;<br>6. exercício regular de direitos em processos judiciais, administrativos ou arbitrais;<br>7. proteção da vida ou da incolumidade física;<br>8. tutela da saúde;<br>9. legítimo interesse; e<br>10. proteção do crédito. | 1. consentimento;<br>2. obrigação legal;<br>3. políticas públicas;<br>4. estudos por órgão de pesquisa;<br>5. exercício regular de direitos, inclusive em contrato e em processos;<br>6. proteção da vida ou da incolumidade física; e<br>7. tutela da saúde, em procedimento realizado por profissionais da saúde; e<br>8. garantia de prevenção à fraude e à segurança do titular. |

Em outras palavras, a LGPD estabeleceu que o consentimento específico e destacado do titular, para finalidades específicas, deve ser buscado para o tratamento de dados sensíveis, por exemplo: pessoa que concorda voluntariamente em participar de uma pesquisa clínica ou paciente que consente em compartilhar os seus dados de saúde como histórico médico entre diferentes profissionais.

Todavia, isso não deve significar que o consentimento específico e destacado deve ser buscado a todo custo. É necessário um exercício de ponderação entre o esforço para obter o consentimento e o benefício e ganho que o tratamento de dados trará para o titular, o controlar e, até mesmo, um terceiro, como a sociedade.

As demais bases legais disponíveis para o tratamento de dados sensíveis só poderiam ser aplicadas na impossibilidade de obtenção de consentimento e exclusivamente quando o tratamento for **indispensável** para as finalidades descritas na LGPD, conforme exemplos abaixo:

- Para cumprimento de obrigação legal ou regulatória pelo controlador, como por exemplo a guarda de prontuários médicos de pacientes, incluindo resultados de exames diagnósticos armazenados eletronicamente em meio óptico, microfilmado ou digitalizado, por 20 (vinte) anos, a partir do último registro no prontuário eletrônico, conforme art. 6º da Lei nº 13.787/2018;

- Para tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, como por exemplo, desenvolvimento de políticas públicas de prevenção ao combate de uma doença epidemiológica; realização de estudos para promoção de campanhas de vacinação em massa; e o compartilhamento da base de dados do Cadastro de Pessoas Físicas pela Secretaria da Fazenda Nacional com a ANS, visando o enriquecimento e melhoria da qualidade dos cadastros de beneficiários;

- Para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados sensíveis, como por exemplo, estudo sobre os efeitos de determinada medicação em pacientes com uma condição médica específica;

- Para o exercício regular de direitos em contratos e processos judiciais, administrativos ou arbitrais, como por exemplo, assinatura de contrato para contratação de planos individuais e prestação de serviços médico hospitalares; contestação de fraude em Declaração de Saúde para fins de encerramento unilateral do contrato de plano privado de assistência à saúde;

- Para proteção da vida ou da incolumidade física do titular ou do terceiro, como por exemplo para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Nesse sentido, a LGPD traz regras para o tratamento desses dados, sejam eles dados pessoais ou dados sensíveis. Abordaremos nos tópicos seguintes as principais regras que as organizações da área da saúde precisam ter em mente no tratamento de tais dados.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 2. Como deve ser o consentimento para o uso de dado de saúde?

**Caso:** Uma empresa de exames médicos coleta o consentimento de seus clientes por meio de um Termo de Consentimento de uma folha, escrito em linguagem jurídica e com as finalidades do tratamento descritas como "desenvolvimento de nossas atividades" e "promoção do seu bem-estar". O representante da empresa busca saber se o seu Termo de Consentimento está adequado à LGPD.

O consentimento para o tratamento de dados pessoais de saúde, classificados como sados sensíveis[9] pela LGPD, é a principal hipótese legal que permite o tratamento desse tipo de dado, sendo as demais bases legais exceções ao consentimento permitidas em situações específicas previstas pela lei[10].

Nesse sentido, uma das principais dúvidas das empresas e profissionais de saúde é a forma como esse consentimento deve ser obtido dos pacientes (titulares dos dados).

A preocupação com a forma é importante, pois a lei busca proteger e empoderar o titular, para que ele tenha um mínimo de controle sobre "se", "como" e "quando" seus dados serão utilizados, especialmente por se tratar de dados potencialmente críticos e discriminatórios que podem ser usados tanto de forma positiva quanto abusiva.

[9] Tema 1 deste guia.
[10] Tema 2 deste guia.

A LGPD define como deve ser obtido o consentimento para dados sensíveis, incluindo dado de saúde por meio de uma série de requisitos que devem ser postos em prática pelo responsável pelo tratamento: **(i) livre; (ii) informado; (iii) inequívoco; e (iv) para finalidades específicas e destacadas.** Esses termos possuem significados distintos que afetam a qualidade do consentimento obtido. Desse modo, explicamos a seguir o significado de cada um[11]:

I. **Livre:** refere-se a um ato do titular que não foi realizado por meio de coação física, moral, psicológica ou artifício que o induza. Trata-se de uma escolha efetiva por parte do titular, com a opção de simplesmente não consentir, mesmo que isso tenha um impacto na sua vida, o que deve ser previamente informado. Um exemplo interessante é a dificuldade de obter um consentimento livre no tratamento de dados de empregados por empregadores, devido à relação de hipossuficiência entre o empregado e o empregador, que pode afetar sua liberdade de optar por não autorizar o tratamento de seus dados;

II. **Informado:** informa o titular sobre a coleta, uso e compartilhamento de seus dados pessoais de forma clara e de fácil entendimento;

III. **Inequívoco:** esta característica enfatiza a necessidade de uma confirmação assertiva da vontade do titular de autorizar o tratamento de seus dados, exigindo sua participação ativa para confirmar que ele entende que seus dados serão tratados para uma finalidade específica. Por exemplo, limita autorizações que abrangem muitas finalidades de uma vez só, especialmente aquelas que podem ter um impacto no indivíduo;

IV. **Finalidades específicas e destacadas:** refere-se à necessidade de uma clara demonstração das finalidades do tratamento dos dados, não sendo permitidas autorizações genéricas ou usos que fujam do contexto do tratamento. Por exemplo, um exame médico pode ter a finalidade tanto de fornecer um diagnóstico para o paciente quanto de utilizar as informações para desenvolvimento de novos medicamentos, entre outros usos.

[11] BIONI, Bruno. Xeque-Mate – O Tripé da Proteção de Dados Pessoais no Jogo de Xadrez das Iniciativas Legislativas nos Brasil. Grupo de Estudos em Políticas Públicas em Acesso à Informação da USP (GPOPAI). Projeto de Pesquisa Financiado pela Fundação Ford. São Paulo: 2015. pp. 45-47. Disponível em: <https://bit.ly/2MObQLD>. Acessado em 05/02/2019.

Também, tem-se dado ênfase à ideia de "consentimento ativo", no qual não seria possível obter o consentimento de forma implícita, pela mera inação do titular dos dados em não se opor ao tratamento, ou pelo seu uso reiterado de determinado serviço.[12]

Assim, um consentimento verdadeiramente ativo busca incentivar o engajamento direto do titular, bem como o fornecimento de informações claras que embasem sua decisão. Como exemplo, pode-se citar a produção de vídeos didáticos, infográficos, configurações de privacidade que permitam ao usuário escolher as finalidades do tratamento de forma personalizada (granular privacy settings), entre outros. Desse modo, o uso exclusivo de longos contratos com linguagem jurídica e de difícil compreensão não seria recomendável.

Também é obrigação do responsável pelo tratamento comprovar que obteve o consentimento de forma adequada, sob pena de o mesmo ser considerado inválido. Além disso, caso haja alteração das finalidades de tratamento, o titular deve ser informado previamente para que seja coletado um novo consentimento.

Por fim, deve-se garantir à pessoa, de forma facilitada, a revogação de seu consentimento, a menos que o controlador consiga fundamentar a continuidade do tratamento por uma das outras bases legais previstas LGPD. No entanto, isso não deve significar que seria possível fundamentar o tratamento simultaneamente em mais de uma base legal.

Ao analisar o exemplo utilizado no início do tópico, verifica-se que as finalidades (i) "desenvolvimento de nossas atividades" e (ii) "promoção do seu bem-estar" podem ser consideradas genéricas, pois não está claro para o titular como as informações serão realmente utilizadas. Uma forma de mitigar esse problema poderia ser com a utilização de exemplos mais específicos, como "envio de SMS com dicas de saúde" e "operacionalização da nossa plataforma online que permite a visualização dos resultados dos exames".

[12] CAROLAN, Eoin. The continuing problems with online consent under the EU's emerging data protection principles. Computer Law and Security Review. Volume 32, Edição 3, junho de 2016. p.5. Disponível em: <https://bit.ly/2JpqFle>. Acessado em: 05/02/2019.

Assim, as finalidades se tornam mais claras, específicas e determinadas. Em relação a linguagem do documento, seria recomendável acrescentar um infográfico que traduzisse a linguagem jurídica do Termo de Consentimento, garantido assim que o consentimento seja devidamente informado. Para qualificar o consentimento como livre, é recomendável fornecer treinamento aos funcionários para evitar qualquer tipo de coação ou imposição, pois a simples exigência de assinatura sem explicações fundamentadas, sem a possibilidade de discordar do tratamento, ou a ausência de esclarecimento de dúvidas podem violar a livre manifestação de vontade.

Por fim, a obtenção de um consentimento específico pode ser alcançada com a assinatura do titular, ou o seu aceite de forma separada, após as qualificações acima terem sido devidamente atendidas. É importante registrar todo esse processo por questões de accountability, uma vez que cabe ao controlador comprovar que obteve de forma adequada o consentimento.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 3. Anonimização e pseudonimização

**Caso:** Uma empresa tradicional do setor de saúde deseja utilizar a base de dados de exames clínicos que já possui, para compartilhar com uma indústria farmacêutica com o objetivo de criar e comercializar novos medicamentos e tratamentos. Contudo, a empresa acredita que o consentimento dado para a realização dos exames clínicos não a autoriza a compartilhar os dados com a indústria farmacêutica para as finalidades pretendidas por ela. Considerando isso, como a empresa poderia viabilizar o desenvolvimento de novos medicamentos e tratamentos por meio do uso dos dados que possui?

A empresa pretende, a partir dos dados coletados de seus pacientes para a realização de exames clínicos, compartilhar os dados com a indústria farmacêutica para que ela desenvolva e comercialize novos medicamentos e tratamentos de saúde.

Em respeito aos princípios da finalidade e da adequação, descritos na Lei Geral de Proteção de Dados, todo e qualquer tratamento de dados pessoais deve ser compatível com as finalidades para as quais os dados pessoais foram originalmente coletados. De acordo com o princípio da finalidade[13] , o tratamento de dados pessoais deve ser feito para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedada a possibilidade de tratamento posterior de forma incompatível com o que foi informado ao titular. Já o princípio da adequação[14] dispõe que o tratamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular e de acordo com o contexto do tratamento.

[13] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso I.
[14] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso II.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

Além disso, a LGPD restringe o compartilhamento de dados de saúde com objetivo de obter vantagem econômica, caso esse compartilhamento não seja para a prestação (i) de serviços de saúde; (ii) de assistência farmacêutica e de (iii) assistência à saúde, incluindo serviços auxiliares de diagnose e terapia; ou para realizar portabilidade, a pedido do titular, e permitir as transações financeiras e administrativas[15].

Desta forma, a princípio, poderíamos dizer que a empresa não poderia, na forma pretendida, por meio simplesmente da base legal que legitimou o tratamento anterior, realizar o compartilhamento dos dados pessoais dos pacientes com a indústria farmacêutica, na medida em que tais dados foram coletados com a finalidade de o paciente realizar os exames clínicos[16].

Contudo, para viabilizar o negócio da empresa e o desenvolvimento e a comercialização de novos medicamentos e tratamentos pela indústria farmacêutica, é possível se valer de metodologias de anonimização, observados os critérios e mecanismos mencionados a seguir.

O artigo 12 da LGPD, inserido na seção específica de dados pessoais sensíveis, afirma expressamente que dados anonimizados não serão considerados dados pessoais para os fins da referida Lei, salvo quando o processo de anonimização puder ser revertido por meios próprios ou com esforços razoáveis.

Para determinação do que é razoável, a LGPD dispõe que deve ser levado em consideração fatores objetivos como, o custo dispendido para a realização do processo de anonimização e o tempo necessário para reverter tal processo, ponderando as tecnologias disponíveis no momento, bem como exclusivamente os meios próprios cabíveis ao agente de tratamento[17].

Ou seja, dados anonimizados são aqueles que não permitem mais identificar o titular a quem originalmente se referiam, utilizando meios técnicos razoáveis e disponíveis na época de seu tratamento. Por esse motivo, eles não são considerados dados pessoais para fins da lei, à exceção de quando forem utilizados para o desenvolvimento de perfis comportamentais de determinada pessoa natural, se identificada[18].

[15] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º, §4º.
[16] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 15º, inciso I.
[17] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 12º, §1º.
[18] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 12º, §2º.

A impossibilidade de identificação do titular retira os dados anonimizados do escopo de aplicação da LGPD. Desta forma, quando são utilizados dados efetivamente anonimizados, não é necessário, por exemplo: (i) obter consentimento do titular ou se fundamentar em qualquer outra base legal que justifique seu tratamento; (ii) reter os dados por um período limitado; (iii) conceder os direitos de informação, de acesso, retificação e eliminação dos titulares; entre outros.

Por exemplo, a Agência Europeia de Medicamentos ("EMA"), que é uma agência descentralizada da União Europeia responsável pela avaliação científica, supervisão e monitoramento da segurança dos medicamentos, realiza a publicação de relatórios clínicos com dados anonimizados para (i) evitar a duplicação de ensaios clínicos, fomentar a inovação e incentivar o desenvolvimento de novos medicamentos; (ii) construir confiança pública e confiança nos processos científicos e de tomada de decisão da EMA; e (iii) fins acadêmicos e de pesquisa para reavaliar dados clínicos[19].

A EMA desenvolveu orientações para a indústria para a publicação de relatórios clínicos, que devem ser obrigatoriamente anonimizados, com técnicas específicas para dados de saúde, para impedir que pacientes e profissionais sejam identificados, a fim de cumprir a legislação europeia sobre proteção de dados pessoais[20]. Inclusive, nessas orientações, a EMA ressalva a complexidade envolvida na anonimização de relatórios clínicos no caso de doenças raras e pequenas populações, devido ao número muito reduzido de pessoas, o que pode levar a reidentificação destas.

No Brasil, a Resolução nº 738/2024 do Conselho Nacional de Saúde (CNS), que dispõe sobre uso de bancos de dados com finalidade de pesquisa científica envolvendo seres humanos, exige a anonimização ou pseudonimização de dados quando houver necessidade justificada do controlador do banco de dados de lhe dar acesso ou transferir a terceiros. Essa anonimização, por

[19] European Medicines Agency. Clinical Data Publication. Acessado em 08/05/2024. Disponível em: <https://www.ema.europa.eu/en/human-regulatory/marketing-authorisation/clinical-data-publication>

[20] European Medicines Agency. External guidance on the implementation of the European Medicines Agency policy on the publication of clinical data for medicinal products for human use. Acessado em 08/05/2024. Disponível em: <https://www.ema.europa.eu/documents/regulatory-procedural-guideline/external-guidance-implementation--european-medicines-agency-policy-publication-clinical-data_en-3.pdf>

outro lado, isenta o controlador de diversas obrigações, incluindo garantir o acesso aos dados pessoais ou obter o consentimento prévio dos participantes da pesquisa.

Portanto, observados os critérios acima mencionados e sendo os dados efetivamente anonimizados, não seria necessária a fundamentação do tratamento em uma base legal adequada para uma finalidade específica, tornando livre o uso dos dados por parte da empresa para os fins desejados. Assim, seria permitido o compartilhamento de tais dados com a indústria farmacêutica, como pretendido pela empresa, e/ou outros stakeholders, sendo até mesmo permitida a análise de tais dados para que sejam extraídas outras informações, como de *business intelligence*.

Também não haveria a restrição a determinados casos para o compartilhamento com o intuito de obter vantagem econômica, por se tratar de dados anonimizados, o que diminuiria os riscos regulatórios para o desenvolvimento do produto pretendido pela empresa e pela indústria farmacêutica. Portanto, tais dados, mesmo anonimizados, podem ser úteis e ter um alto valor para o mercado.

Vale lembrar que a pseudonimização e a anonimização não podem ser confundidas.

Dados pseudonimizados são aqueles que impossibilitam a associação a um indivíduo, salvo pelo uso de informação adicionalmente mantida em separado pelo controlador.

Dados pseudonimizados ainda são dados pessoais, uma vez que possibilitam a reidentificação do titular dos dados a partir de informações adicionais, devendo, portanto, atender às obrigações legais relativas à essa matéria, como o tratamento somente após a obtenção de uma base legal adequada. De toda forma, é certo que tais dados ajudam a minimizar os riscos do tratamento dos dados pessoais, diminuindo, inclusive, a probabilidade de identificação de uma pessoa.

Sendo assim, para que seja realizado o compartilhamento de dados de saúde com a indústria farmacêutica com o objetivo de se desenvolver novos medicamentos e tratamentos, a orientação é que os dados sejam efetivamente anonimizados, sendo vedada a possibilidade de reversão desse processo, considerando o custo, o tempo e as tecnologias disponíveis.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 4. Hipóteses legais que permitem o compartilhamento de dados de saúde

**Caso:** Uma empresa, especializada na venda de comida online, busca explorar novos negócios a partir da comercialização de seus dados, inclusive dados referentes aos hábitos de consumo (como frequência e os tipos de comida compradas) a empresas de planos e seguros de saúde (serviços de saúde suplementar). Com tais dados, estas podem avaliar a saúde de seus clientes e, até mesmo, cobrar prêmios diferenciados com base nos riscos encontrados. Todavia, a empresa gostaria de saber sobre a legalidade de tal prática e qual base legal poderia lhe autorizar a compartilhar tais dados.

A empresa pretende, a partir dos dados obtidos em seu aplicativo de venda de comida online, comercializar dados que permitem empresas de planos e seguros de saúde inferir hábitos de consumo de seus usuários, possibilitando que estas façam a avaliação dos riscos à saúde de seus clientes e consequentemente a cobrança de prêmios diferenciados.

Em primeiro lugar, qualquer tratamento de dados pessoais deve ser compatível com as finalidades para as quais os dados pessoais foram coletados originalmente, e conforme informado ao titular dos dados, neste caso, aos usuários do aplicativo da empresa no momento de sua instalação.

Segundo, de acordo com o princípio da finalidade[21] , o tratamento de dados pessoais deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular. É vedado o tratamento posterior de forma incompatível com o que foi informado ao titular. Já o princípio da adequação[22] dispõe que o tratamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular e de acordo com o contexto do tratamento.

Além disso, importante observar que possivelmente tais dados serão interpretados como dados sensíveis, pois podem inferir informações sobre a saúde do titular, pois serão tratados para a avaliação dos riscos à saúde dos titulares.

No caso em questão, considerando que o aplicativo é especializado na venda de comida online, é possível que os dados referentes aos hábitos de consumo do usuário, além daqueles necessários para fazer os pedidos, como dados de pagamentos e histórico de entregas, estejam sendo coletados para aprimorar os serviços e a experiência do usuário na plataforma. Sendo assim, tratamentos secundários dos dados, como a comercialização destes e avaliação dos riscos dos titulares por empresas de planos e seguros de saúde, podem não ser considerados compatíveis com os fins para os quais os dados foram originalmente coletados.

A LGPD autoriza o compartilhamento de dados de saúde com objetivo de obter vantagem econômica podendo ser feito apenas quando[23] for realizado para a prestação de serviços de saúde, assistência farmacêutica e assistência à saúde, desde que em benefício dos interesses dos titulares.

Ademais, não é permitido que as operadoras de planos privados de assistência à saúde realizem tratamento de dados de saúde para (i) realizar seleção de riscos na contratação de qualquer modalidade, e (ii) contratar e excluir beneficiários[24].

Entretanto, os termos utilizados para descrever as hipóteses de compartilhamento podem ser considerados bastante amplos. Nesse sentido, é possível que Autoridade Nacional de Proteção de Dados Pessoais possa vir a regular de

[21] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso I.
[22] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso II.
[23] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, §4º.
[24] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, § 3º.
[25] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, § 3º.

forma mais específica determinados setores do ecossistema de saúde privada[25]. Por exemplo, será que o ganho de eficiência em tratamentos, o oferecimento ao titular de outros serviços, ou até mesmo o ganho em custos de todo o ecossistema podem ser consideradas finalidades para as quais o compartilhamento de dados esteja relacionado à prestação de serviço de saúde? É igualmente difícil obter parâmetros de autoridades de proteção de dados estrangeiras, pois esse dispositivo existe apenas na legislação brasileira. A ANPD terá um papel fundamental na elucidação de tais dúvidas, que antes de serem dirimidas, devem ser analisadas por meio de exercícios de colaboração entre diferentes órgãos reguladores, como a ANS, representantes da iniciativa privada e entidades do terceiro setor.

Por fim, em relação ao caso apresentado no início do tópico, dificilmente o compartilhamento de dados na forma pretendida seria considerado legítimo, mesmo com o consentimento específico do titular, sob o argumento que isso poderia lhe trazer benefícios, como o barateamento dos seus custos com serviços de saúde suplementar por ser este uma pessoa com hábitos alimentares saudáveis. Nota-se uma violação aos princípios gerais, como o da finalidade e adequação. Ainda, tal caso dificilmente seria interpretado como uma das hipóteses que autorizam o compartilhamento de dados de saúde com o objetivo de obtenção de vantagem econômica.

No entanto, potencialmente seria possível utilizar esses dados de forma anonimizada, visando entender os hábitos gerais de um determinado grupo, desde que os dados agrupados não sejam atribuídos a indivíduos identificados.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 5. Direitos dos titulares dos dados:

## *definição e limitações legais*

**Caso:** Um determinado paciente realizou por 25 anos suas consultas médicas e exames clínicos em determinado hospital. Ao mudar de convênio de saúde, o paciente perdeu a cobertura naquele hospital, passando a realizar seus exames e acompanhamento médico em um outro estabelecimento de saúde. Sabendo que a Lei Geral de Proteção de Dados criou os direitos de portabilidade e de exclusão dos dados pessoais, o paciente enviou requerimento ao seu antigo hospital, solicitando a portabilidade de seus dados para o novo e, em seguida, requerendo que seus dados no antigo fossem excluídos. Pergunta-se: o hospital pode manter os dados?

O caso apresentado acima envolve uma questão de direitos dos titulares dos dados. Essa é uma questão relevante, pois a LGPD conferiu aos titulares uma série de direitos com o intuito de oferecer-lhes mecanismos para um maior controle sobre seus dados.

Nesse sentido, a LGPD garante os seguintes direitos para os titulares[26]:

1. confirmação da existência de tratamento;
2. acesso aos dados;
3. correção de dados incompletos, inexatos ou desatualizados;
4. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
5. ortabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial;
6. eliminação dos dados tratados com o consentimento do titular;
7. informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
8. informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
9. revogação do consentimento; e
10. revisão de decisão automatizada.

Ocorre que esses direitos não são absolutos. Por exemplo, existem hipóteses previstas pela LGPD em que a empresa poderia não eliminar os dados[27], sendo permitida a manutenção para atender às seguintes finalidades:

[26] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, I a IX e Artigo 20.
[27] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 16, I a III.

1. cumprimento de obrigação legal ou regulatória pelo controlador;
2. estudo por órgão de pesquisa[28], garantida, sempre que possível, a anonimização dos dados pessoais;
3. transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; e
4. uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Aplicando os conceitos expostos acima, temos: o paciente, titular dos dados pessoais, requerendo a portabilidade e exclusão de seus dados pessoais ao hospital antigo que, no caso, seria o controlador desses dados.

I. Quanto ao direito de portabilidade: em razão da requisição expressa do titular, o hospital antigo precisará transferir os dados do paciente para o hospital novo de forma interoperável[29] , não havendo obrigação de transferência em relação aos dados eventualmente anonimizados[30]. Cumpre pontuar que ainda não existem padrões oficialmente definidos sobre interoperabilidade, os quais devem ser futuramente estabelecidos pela ANPD. Ainda, critérios de proporcionalidade podem ser aplicados, como custo, tempo e existência de padrões que permitam a interoperabilidade entre os sistemas dos diferentes controladores;

II. Quanto ao direito de exclusão: os dados contidos em prontuário médico (em meio eletrônico ou físico) obtidos há mais de 20 anos deverão ser excluídos da base de dados do hospital antigo, em razão da requisição do titular desses dados. Contudo, os dados de prontuários médicos com até 20 anos devem ser mantidos pelo hospital, em razão de obrigação legal imposta pela Lei nº 13.787/2018[31]. Outros dados que não estão em prontuário médico também devem ser excluídos, caso não exista uma base legal que permita sua manutenção.

[28] "Órgão de Pesquisa" é definido no artigo 5º, XVIII, da LGPD como ***"órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos*** legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico".

[29] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 40.
[30] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, § 7º.
[31] BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Artigo 6º.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

Portanto, ainda que os direitos dos titulares não sejam absolutos, uma vez em que há exceções em que os agentes de tratamento não precisam cumpri-los como, por exemplo, não eliminação dos dados em caso de necessidade de cumprimento de obrigação legal ou regulatória, é preciso que as empresas do setor de saúde desenvolvam mecanismo para garantir que os titulares possam exercer seus direitos. Já existem no mercado algumas ferramentas como plataformas de gerenciamento de dados, os chamados "Privacy Dashboards". Desta forma, necessário adequar os sistemas e práticas existentes aos padrões de interoperabilidade e formas de cumprir com as requisições de direitos previstos na LGPD.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 6. Dados de saúde de funcionários

**Caso:** Uma empresa, que atua no setor de Engenharia e Construção, pretende realizar o controle e monitoramento dos smartphones utilizados por seus funcionários. A empresa, contudo, não oferece smartphones corporativos, e os funcionários utilizam dispositivos pessoais para exercer suas funções. Além de coletar dados de geolocalização, a empresa pretende coletar dados que permitem aferir se o funcionário pratica exercícios físicos ou não, na sua rotina, com o objetivo de oferecer plano de saúde empresarial coletivo a seus colaboradores, adequado aos seus hábitos. Para tanto, a empresa questiona sobre a legalidade da coleta de tais dados, bem como a base legal que a justificaria.

A empresa pretende, a partir dos dados coletados através do smartphone de seus funcionários, coletar dados que permitam aferir se o funcionário pratica exercícios físicos ou não na sua rotina, com a finalidade de oferecer plano de saúde empresarial coletivo a seus colaboradores modelados aos seus hábitos.

Primeiramente, vale lembrar que dado de saúde deve ser compreendido como todo dado que estiver estritamente ligado ao estado de saúde de uma pessoa[32], ou permita inferir tal estado. Sendo assim, considerando que os dados pretendidos pela empresa podem gerar inferências sobre o estado de saúde do funcionário, aferindo se o funcionário pratica ou não exercícios, tais dados podem ser considerados sensíveis, haja vista, ainda, o contexto do tratamento da empresa[33].

A legislação trabalhista brasileira, como a Consolidação das Leis do Trabalho (a Lei nº 5.452/1943) e portarias emitidas pelo Ministério do Trabalho e Emprego, estabelecem obrigações específicas em relação aos dados pessoais de empregados.

[32] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records, 15 February 2007.
[33] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso II.

Como se sabe, para cumprimento do contrato de trabalho e de determinadas exigências legais, algumas informações sobre os funcionários deverão ser obrigatoriamente coletadas pelo empregador, como:

I. os arquivos de registro de funcionários, que contêm dados pessoais e profissionais relacionados a cada empregado, onde constam informações como nome, endereço, data e local de nascimento, estado civil, nomes dos pais, profissão, país de nascimento, número da CTPS, do CPF, do RG, do título de eleitor e do número do PIS, data de início do emprego, função e salário do empregado, entre outras;

II. relatórios atualizados de saúde e segurança (como PCMSO, PPRA e PPP, entre outros), que mostram o trabalho realizado pelo funcionário do ponto de vista de saúde e segurança do trabalho; e

III. informações a serem enviadas ao Governo, como registros sobre a folha de pagamento, horas extras, férias e outras obrigações trabalhistas, previdenciárias e tributárias ('e-Social') sobre o empregado.

Adicionalmente, a jurisprudência da justiça do trabalho estabeleceu algumas regras e diretrizes a respeito da privacidade e a proteção de dados pessoais no ambiente de trabalho, fixando os limites do empregador no contexto laboral quando houver, por exemplo, o monitoramento e vigilância do empregado; a utilização de equipamentos e sistemas de tecnologia da informação; o uso de sistemas de vigilância no ambiente de trabalho; e a verificação de antecedentes criminais e financeiros.

Com relação ao **monitoramento,** que é o caso em questão, a maioria das decisões dos tribunais superiores sobre este assunto sustentam a posição de que os empregadores estão autorizados a monitorar o uso de sistemas de equipamentos disponibilizados para funcionários, sem que isso configure violação do direito à privacidade, desde que os funcionários sejam informados com antecedência sobre todas as atividades de monitoramento realizadas pelo empregador (o que pode ser feito através de políticas e avisos internos de privacidade e segurança da informação da empresa).

Ainda, é necessário que o empregador faça tal monitoramento **visando a boa prestação dos serviços** de seus funcionários, sempre de maneira **razoável e proporcional,** para que isso não seja interpretado como abuso do poder diretivo ou como interferência na vida privada ou na intimidade dos colaboradores. Ainda nesta seara, o monitoramento deve se restringir às atividades laborais, sendo vedada a observação de atividades da vida privada, como e-mail pessoal ou redes sociais, mesmo quando acessadas por meio de equipamentos corporativos, salvo em casos de evidenciadas suspeitas de conduta inadequada.

Pós-pandemia tornou-se mais comum, por exemplo, o uso de dispositivos pessoais no ambiente corporativo, considerando o crescimento do trabalho em modalidade *home office.* O monitoramento desses tipos de dispositivos, sobretudo fora do horário de trabalho, contudo, excede as fronteiras das atividades laborais e configura uma prática desproporcional e invasiva à esfera privada do colaborador.

Além disso, algumas **regras adicionais** deverão ser observadas pelas companhias quando forem tratados dados pessoais de seus empregados. De acordo com a LGPD[34], para coletar, processar, armazenar e divulgar um dado pessoal de um empregado, o empregador deverá (i) observar os **princípios** trazidos pela LGPD ; (ii) ter uma **base legal** que justifique o tratamento de dados pessoais e/ou sensíveis de seus empregados[35] ; (iii) cumprir com os **direitos dos titulares de dados**[36]; dentre outras obrigações.

Como dito anteriormente, os dados utilizados pela empresa no caso concreto são dados que geram inferências sobre a saúde do empregado, exigindo que a empresa se valha de hipóteses legais especificas para seu tratamento.

Uma das bases legais que possibilita o tratamento de dados sensíveis de acordo com a LGPD é o **consentimento** do titular (no caso, o funcionário), que deve ser l**ivre**, **informado e inequívoco**, bem como realizado de forma **específica e destacada**[37]. No entanto, para que o consentimento seja livre, é necessário que exista uma escolha real por parte do titular dos dados (funcionário), se este deseja ou não concordar com o tratamento dos seus dados e sem que haja penalidade substancial caso o funcionário se oponha ao tratamento.

[34] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 6º, incisos I a X.
[35] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigos 7º e 11º.
[36] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 9º.
[37] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11.

Dado o desequilíbrio existente na relação empregador/empregado, é pouco provável que o funcionário possa negar seu consentimento ao empregador para o tratamento de seus dados pessoais sem que experimente o medo ou o risco de efeitos prejudiciais causados pela recusa. Além disso, ainda que fornecido o consentimento, parece problemática a aparente impossibilidade de o funcionário revogar esse consentimento ou opor-se, de qualquer maneira, ao tratamento dos dados pessoais sem sofrer reveses. Tanto a prerrogativa de informação sobre a possibilidade de negar o consentimento, quanto a de revogá-lo, são direitos garantidos pela LGPD aos titulares de dados[38].

Sendo assim, valer-se da base legal do consentimento para tratamento de tais dados sensíveis no contexto em questão **pode ser considerado problemático**, uma vez que é improvável que o consentimento seja dado de forma livre pelo funcionário.

Como se não bastasse, a coleta de tais dados pela empresa também **desafia o princípio da necessidade,** que limita o tratamento dos dados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Isso, sem falar da possível incompatibilidade com os **princípios da finalidade e da não discriminação,** considerando as dúvidas postas à própria licitude da atividade na forma pretendida pela empresa.

Portanto, no caso em questão, provavelmente **não** seria recomendado que a empresa realize a coleta dos dados que permitem aferir se o funcionário pratica exercícios físicos ou não através de seu smartphone, pois **(i)** a coleta de tais dados pode vir a ser interpretada como abuso do poder diretivo ou como interferência na vida privada ou intimidade dos colaboradores, na medida em que são coletados fora do escopo do trabalho e sem relação aos serviços prestados; e **(ii)** tal prática desafia princípios da LGPD, podendo ser incorrer em coleta excessiva, além de possivelmente não possuir uma base legal segura que legitime o tratamento de tais dados.

A prática mais recomendada para prosseguir com o monitoramento seria adequá-lo aos princípios e fundamentos da LGPD, por meio, por exemplo, do fornecimento de um dispositivo corporativo ao funcionário; da garantia de transparência por políticas e procedimentos sobre o uso de dispositivos corporativos; da limitação da frequência do monitoramento e dos tipos de informações monitoradas, adequando-as às legítimas expectativas do ambiente de trabalho; e da atribuição de uma base legal mais adequada.

[38] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, VIII e IX.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

**Caso:** Um hospital privado em Minas Gerais detectou uma invasão em seu banco de dados, tendo sido acessados laudos eletrônicos de alguns de seus pacientes contendo diversos dados sensíveis, como histórico familiar de doenças, diagnósticos realizados, histórico de internações e medicamentos utilizados. Nesse sentido, o hospital busca saber quais ações ele deve adotar perante os consumidores afetados e as autoridades competentes e quais serão as possíveis sanções a ele aplicadas.

No caso de descumprimento das normas referentes ao tratamento de dados pessoais, sejam eles sensíveis ou não, a empresa pode sofrer tanto sanções de cunho administrativo, aplicadas principalmente pela Autoridade Nacional de Proteção de Dados (ANPD), quanto ser condenada por tribunais. Para além da ANPD, é interessante notar que os organismos de defesa do consumidor, como os Procons do Ministério Público, também devem ter atuação importante na fiscalização da LGPD, principalmente porque os titulares dos dados pessoais podem peticionar seus direitos em ambas as instituições.[39]

As categorias de responsabilização citadas acima podem ocorrer de forma concomitante, não sendo mutuamente excludentes[40]. Assim, por exemplo, se um hospital privado compartilha dados sensíveis de saúde com uma instituição bancária a fim de obter ganhos financeiros, o que não se enquadra nas hipóteses de compartilhamento de dados de saúde com fins de obtenção de vantagem econômica[41], ele pode ser sancionado tanto pela ANPD quanto ser processado pelos pacientes, os quais podem buscar indenizações por danos materiais e/ou morais.

[39] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18. Parágrafo 8º.

O art. 52 da Lei Geral de Proteção de Dados, dispõe sobre quais são as sanções administrativas aplicáveis pela ANPD para qualquer infração às regras de tratamento de dados pessoais:

" I. - advertência, com indicação de prazo para adoção de medidas corretivas;
II. - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III. - multa diária, observado o limite total a que se refere o inciso II;
IV. - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V. - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. - eliminação dos dados pessoais a que se refere a infração;" [grifo nosso]

No caso de uma possível infração, a ANPD terá a prerrogativa de iniciar um processo administrativo, no qual o acusado possui direito à ampla defesa, nos termos do Regulamento de Fiscalização da Autoridade.[42] Na análise de qualquer caso, a LGPD exige que sejam considerados os seguintes elementos:

" I. a gravidade e a natureza das infrações e dos direitos pessoais afetados;
II. - a boa-fé do infrator;
III. - a vantagem auferida ou pretendida pelo infrator;
IV. - a condição econômica do infrator;
V. - a reincidência;
VI. - o grau do dano;
VII. - a cooperação do infrator;
VIII. - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados [...];
IX. - a adoção de política de boas práticas e governança;
X. - a pronta adoção de medidas corretivas; e
XI. - a proporcionalidade entre a gravidade da falta e a intensidade da sanção."

[40] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 52. Parágrafo 2º.
[41] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11. Parágrafo 4º.

A fim de regulamentar esses parâmetros, a ANPD criou um Regulamento de Dosimetria e Aplicação de Sanções Administrativas, que categoriza as infrações à LGPD em leves, médias ou graves e dispõe sobre os procedimentos para a aplicação de cada sanção administrativa, incluindo a metodologia de cálculo do valor das sanções de multa.[43]

Um dos temas de vanguarda da Autoridade é o combate aos incidentes de segurança da informação, incluindo os vazamentos de dados. Entre 2022 e 2023, por exemplo, oito dos nove processos administrativos sancionadores em andamento pela ANPD tratavam de incidentes de segurança da informação, conforme relatado pela Autoridade no Relatório do Ciclo de Monitoramento de 2023.[44]

Em outubro de 2023, por exemplo, a ANPD publicou sanção contra a Secretaria de Saúde do Estado de Santa Catarina (SES-SC), constatando que o órgão violou, entre outras, a obrigação da LGPD de comunicar a autoridade e os titulares de dados em caso de incidente, bem como a obrigação de manter a segurança dos sistemas utilizados para o tratamento de dados pessoais. A SES-SC, na ocasião, havia sofrido um incidente de segurança que expôs as informações de mais de 300.000 pessoas.[45]

No caso exemplificado do vazamento de prontuários médicos do Hospital, a LGPD exige que os consumidores afetados e a Autoridade sejam informados sobre o ocorrido, caso fique constatado que o incidente de segurança pode acarretar risco ou dano relevante aos titulares.

Ademais, na ocasião da definição de eventual sanção, a ANPD avaliaria se o Hospital adotava medidas de segurança adequadas, incluindo, por exemplo, se armazenava os dados sensíveis em formato criptografado com objetivo de dificultar sua utilização.
As circunstâncias do caso poderiam levá-la a aplicar sanções mais brandas, como no caso de o Hospital possuir um robusto programa de governança corporativa de privacidade e

[43] BRAISL. ANPD. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

[44] ANPD. Relatório do Ciclo de Monitoramento. 1º semestre de 2023, p. 28. Dez. 2023. Acessado em: 28/02/2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final.pdf

[45] ANPD. ANPD sanciona mais um órgão público. Out. 2023. Acessado em: 28/02/2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-mais-um-orgao-publico.

proteção de dados, com políticas adequadas e implementadas, além de ter contribuído com as investigações. Desse modo, os detalhes técnicos explicando os motivos do vazamento e a postura do Hospital durante e após o incidente são de suma importância para a análise da ANPD e para a medição das sanções aplicáveis.

Por fim, nesse cenário os consumidores também poderão exigir indenizações na própria Justiça, seja em processo individual ou coletivo, se devidamente comprovado o nexo causal com o incidente. Assim, a adoção de medidas de segurança adequadas, |apesar de não afastarem eventuais indenizações por dano moral ou material por vazamento, são consideradas como um elemento essencial, por exemplo, para diminuir o valor de eventual multa.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 8. Melhores práticas de proteção de dados para dados de saúde

**Caso:** Uma empresa cujo modelo de negócio é a comercialização de testes genéticos, está desenvolvendo um aplicativo que permitirá aos seus usuários acessar rotinas de saúde personalizadas com base nos resultados de seus testes. Reconhecendo a importância da proteção dos dados pessoais dos usuários, a empresa busca orientação para implementar as melhores práticas existentes de proteção de dados desde a fase inicial do desenvolvimento do aplicativo.

A LGPD estabelece a obrigação de implementar medidas de segurança, abrangendo tanto aspectos técnicos quanto administrativos, desde a concepção até a execução de produtos ou serviços. Esta responsabilidade legal destaca a importância de integrar a privacidade e a proteção de dados em todas as etapas do desenvolvimento de produtos e serviços.

Em particular, no âmbito do desenvolvimento de produtos e serviços relacionados ao tratamento de dados de saúde, a implementação destas medidas assume uma relevância ainda maior. Isso ocorre devido à natureza altamente sensível das informações manipuladas e aos riscos potenciais inerentes a qualquer falha na salvaguarda desses dados.

O caso acima envolve as melhores práticas que podem ser adotadas por uma empresa que ao desenvolver um aplicativo que trata dados genéticos. No caso do tratamento de dados genéticos, existem riscos que são inerentes à essa atividade. Em relatório, o *Future of Privacy Forum*[46] cita alguns deles:

I. possibilidade de identificar predisposições e risco de doenças;

II. possibilidade de revelar informações sobre os membros da família além do indivíduo que realiza o teste;[47]

III. possibilidade de revelar informações inesperadas cujo impacto pode não ser entendido no momento da coleta;
entre outros.

O capítulo VII da Lei Geral de Proteção de Dados é divido em duas partes: uma seção sobre **segurança e sigilo de dados**[48] e outra seção sobre **governança e boas práticas**[49]. O propósito das normas de segurança e sigilo dos dados é a proteção dos Dados Pessoais contra "acessos não autorizados" e "situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", ou seja, refere-se ao campo amplo da segurança da informação *(infosec)*. Já a finalidade da segunda parte é estimular empresas a adotarem regras de boas práticas de proteção de dados e governança em privacidade.

Ocorre que tanto as normas de segurança da informação, quanto de governança e boas práticas não trazem padrões específicos, servindo apenas como uma orientação geral. Isso porque será papel da Autoridade Nacional de Proteção de Dados fixar parâmetros e regras claras para o mercado, preferencialmente por meio de uma participação ativa dos entes regulados.

Assim, hoje, a recomendação das melhores práticas para o tratamento de dados genéticos seria baseada nas regras e princípios gerais de proteção de dados.

Portanto, no caso em questão, é possível afirmar que as seguintes medidas provavelmente seriam classificadas como boas práticas para a empresa:

[46] FUTURE OF PRIVACY FORUM. Privacy Best Practices for Consumer Genetic Testing Services. Washington, Julho 2018. Página 1.
[47] Primeiro caso criminal nos EUA que utilizará family tree forensics: <https://www.wired.com/story/thefirst-murder-case-to-use-family-tree-forensics-goes-totrial/>

[48] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 46 e seguintes.
[49] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 50 e seguintes

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

1. **Anonimização:** conforme explicado em tópicos anteriores, submeter os dados a processos de **anonimização** traz uma **maior segurança** para o tratamento, além de criar novas possibilidades de uso destes dados.

2. **Consentimento:** conforme abordado anteriormente, o consentimento deve ser obtido a partir de uma manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Para dados sensíveis, este precisa ser, ainda, **específico e destacado**. Em se tratando de dados genéticos, caso a empresa deseje utilizar esses dados para outras finalidades (ex.: pesquisa na área da medicina preventiva), será necessário obter um novo consentimento do titular para essas novas finalidades de forma específica. Ainda, é recomendável que o consentimento seja obtido de forma granular[50], por exemplo, de forma separada para as finalidades: de teste genético, de pesquisa e de envio de marketing dos outros produtos da empresa etc.

3. **Política de Privacidade:** o documento deve ser redigido de forma clara, objetiva e acessível. Assim, é importante que a Política de Privacidade seja **completa** e apresente de **forma simples** as informações sobre o tratamento de dados pessoais realizado pela empresa, especialmente no caso de dados genéticos. Para tanto, é recomendável indicar de forma detalhada os dados coletados, suas finalidades, a forma pela qual os titulares poderão exercer os seus direitos, as hipóteses de compartilhamento dos dados, entre outros pontos.

4. **Compartilhamento:** caso seja necessário o compartilhamento de dados com terceiros, a empresa deve estar atenta às regras para o compartilhamento de dados pessoais de saúde descritos anteriormente. Além disso, os contratos firmados com tais terceiros devem estabelecer cláusulas que garantam o tratamento adequado de dados pessoais pelos parceiros, bem como salvaguardem os interesses da empresa e dos titulares.

[50] UNIÃO EUROPEIA. Working Party 29. Opinion 02/2013 on apps on smart devices. Disponível em

5. **Segurança:** o tratamento de dados de saúde exige um alto nível de segurança e confidencialidade. Isso envolve a aplicação de criptografia avançada, auditorias periódicas, proteção contra ameaças cibernéticas, gerenciamento de acesso preciso, treinamento contínuo de conscientização em segurança e um plano eficaz de resposta a incidentes.

Por último, o tratamento deve se valer, a todo momento, do princípio da prevenção, que determina a adoção de medidas para evitar danos, e o da não discriminação, que veda o tratamento de dados para fins discriminatórios ilícitos ou abusivos.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 9. Relatórios de Impacto à Proteção de Dados na área da saúde

**Caso:** Um hospital público está considerando a implementação de soluções de Inteligência Artificial para aprimorar suas práticas de medicina preventiva. Com o objetivo de compreender e mensurar possíveis riscos à privacidade e segurança dos titulares de dados de saúde, o hospital está avaliando a elaboração de Relatórios de Impacto à Proteção de Dados para identificar potenciais impactos do uso da IA no tratamento dessas informações sensíveis.

O Relatório de Impacto à Proteção de Dados (RIPD) é um documento que descreve os processos de tratamento de dados pessoais que podem representar um risco significativo para os direitos e liberdades fundamentais dos titulares de dados[51]. Ele inclui uma análise detalhada das medidas, salvaguardas e mecanismos de mitigação de riscos[52], de forma a assegurar a conformidade com as disposições legais e a proteção eficaz dos dados pessoais.

[51] Autoridade Nacional de Proteção de Dados (ANPD). Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd . Acesso em: 05 de março de 2024.

[52] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigos 5º,XVII e 38.

A LGPD enumera situações específicas em que a ANPD pode exigir a elaboração do RIPD, tais como:

1. operações de tratamento voltadas exclusivamente para segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais[53];
2. tratamento fundamentado na hipótese de interesse legítimo[54];
3. para agentes do Poder Público, incluindo a determinação de publicação do RIPD[55]; e
4. para controladores em geral, quando entender necessário, abrangendo suas operações de tratamento, inclusive aquelas que envolvem dados pessoais sensíveis[56].

Portanto, como prática geral, a elaboração do RIPD é recomendada sempre que as operações de tratamento de dados pessoais apresentarem potencial risco aos direitos e liberdades fundamentais dos titulares de dados[57].

[53] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 4º, § 3º.
[54] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 10, §3º.
[55] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 32.
[56] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 38.

Essa prática está alinhada com o princípio de responsabilização e prestação de contas[58], que demanda que o agente de tratamento esteja atento aos potenciais riscos associados ao tratamento de dados e tome medidas adequadas para mitigar esses riscos. Nessas hipóteses, a elaboração do RIPD torna-se uma ferramenta essencial para avaliar e gerenciar esses riscos de forma eficaz.

Até o momento, não existe regulamento específico da ANPD sobre o RIPD, dessa forma, a Autoridade recomenda que os controladores adotem como referência o conceito de tratamento de alto risco estabelecido no art. 4º do Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte, aprovado pela Resolução nº 2/2022.

Segundo esse dispositivo, o tratamento será considerado de alto risco quando houver a presença de, pelo menos, um critério geral e um critério específico, conforme indicado abaixo:

[57] Autoridade Nacional de Proteção de Dados (ANPD). Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd . Acesso em: 05 de março de 2024.
[58] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 6º, X.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# Tratamento de alto risco

*ART 4º, RES. CD;ANPD nº2;2022*

## 01 Critério geral

Tratamento em larga escala*

OU

Tratamento que possa afetar significantemente interesses e direitos dos titulares**

+

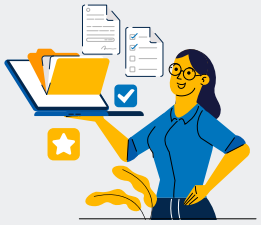
## 01 Critério específico

Vigilância ou controle de zonas acessíveis ao público

OU

Tratamento automatizado

Tecnologias emergentes ou inovadoras



Dados sensíveis ou de crianças, adolescentes e de idosos

No caso acima, percebe-se que o tratamento que o hospital pretende realizar encontra-se na definição de alto risco trazida pelo Regulamento, já que conta com os seguintes critérios:

| CRITÉRIOS GERAIS | CRITÉRIOS ESPECÍFICOS |
|---|---|
| • **Tratamento em larga escala:** Como hospital público, é provável que o tratamento de dados de saúde ocorra em larga escala[59], envolvendo um grande volume de informações e de pacientes.<br>• **Possibilidade de afetar interesses e direitos fundamentais dos titulares:** A depender do tipo de IA utilizada e ferramentas disponíveis, a implementação de soluções de IA para medicina tem potencial de afetar os direitos fundamentais dos pacientes, que podem resultar em impactos negativos para sua saúde e bem-estar. | • **Uso de tecnologias emergentes ou inovadoras:** A depender do tipo de IA utilizada, ela pode ser considerada uma tecnologia emergente e inovadora, o que aumenta a complexidade e os riscos associados ao tratamento de dados de saúde.<br>• **Utilização de dados pessoais sensíveis:** Os dados de saúde dos pacientes são considerados dados pessoais sensíveis pela LGPD, exigindo um cuidado especial em relação à sua proteção e privacidade. |

[59] Conforme a RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022, no artigo 4º, §1º, o tratamento de dados pessoais em larga escala é caracterizado quando envolve um número significativo de titulares, considerando o volume de dados, a duração, a frequência e a extensão geográfica do tratamento.

É importante ressaltar que esses critérios não devem ser considerados exaustivos para a elaboração do RIPD. Cabe ao controlador avaliar as circunstâncias específicas do caso concreto a fim de identificar os riscos envolvidos e adotar medidas adequadas de prevenção e segurança.

Para cumprir com a LGPD, o RIPD elaborado pelo hospital deve conter no mínimo os seguintes requisitos, de acordo com as recomendações da ANPD[60]:

I. a descrição dos tipos de dados tratados;
II. a metodologia utilizada para o tratamento e para a garantia da segurança das informações; e
III. análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Nessa perspectiva, o RIPD serviria para o hospital tanto (i) para auxiliá-lo na adoção de medidas adequadas para estar em conformidade com a lei, quanto (ii) para efetivamente demonstrar que o hospital está em conformidade com a legislação.

[60] Autoridade Nacional de Proteção de Dados (ANPD). Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd . Acesso em: 05 de março de 2024

Vale mencionar que o RIPD não deve ser percebido apenas como uma ferramenta de autorregulação empresarial, mas sim como um instrumento de meta-regulação[61]. Este último conceito, desenvolvido por Christine Parker, teria como consequência exigir que as próprias empresas também sejam responsáveis por verificar sua conformidade com a regulação estatal, reportando suas análises internas às agências reguladoras. Assim, neste caso, a empresa deveria se utilizar de seus próprios recursos e estrutura administrativa para demonstrar estar em conformidade com as leis de proteção de dados pessoais, ao invés de ser apenas um alvo passivo da fiscalização estatal.

Outro ponto interessante de se destacar é que não existe uma única metodologia de produção de um RIPD. Apesar de os objetivos das diversas metodologias serem os mesmos, existem vários *frameworks* diferentes elaborados pelas Autoridades de Proteção de Dados de países europeus, por organizações privadas como a ISO, e modelos desenvolvidos especificamente para analisar determinados produtos e serviços (p. ex. uso de RFID, *smart grids*, entre outros).

[61] BINNS, Reuben. Data Protection Impact Assessments: A Meta-Regulatory Approach. Business Horizons. International Data Privacy Law, Vol. 7(1). 2017.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

A ANPD apenas recomenda a utilização de metodologias reconhecidas como boas práticas pela comunidade técnica. Destaca-se que a decisão sobre a metodologia é responsabilidade do controlador, considerando as possíveis consequências para os titulares, como perda de confidencialidade, uso indevido de dados e violação de direitos.

Por fim, é necessário que um RIPD seja revisado periodicamente, principalmente quando houver alterações significativas na forma do tratamento ou modelo de negócio que tragam novos riscos aos direitos e liberdades dos titulares.

Desse modo, no caso da rede de hospitais que busca implementar um algoritmo de Inteligência Artificial, é fundamental que seja realizado um RIPD no momento anterior à sua aplicação, ou até mesmo ao seu desenvolvimento, para que os riscos sejam avaliados e mitigados de forma adequada, além de facilitar a demonstração de processo de conformidade em futuras fiscalizações da ANPD.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# 10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Caso:** Uma startup brasileira está desenvolvendo um algoritmo de inteligência artificial para diagnosticar problemas de pele, por meio de análise de imagens. Os sócios dessa empresa buscam saber quais regulações da ANVISA lhes são aplicáveis e quais medidas eles devem adotar para estarem em conformidade com a legislação brasileira de proteção de dados pessoais.

Em um primeiro momento deve-se destacar que os diversos tipos de algoritmos de inteligência artificial existentes atualmente referem-se ao conceito de IA[62] no sentido estrito (*narrow AI*), o qual pode ser definido como sistema que possui a capacidade de detectar padrões em um conjunto de dados, aprender com esses dados e usar esse aprendizado para atingir metas e tarefas específicas por meio de uma adaptação flexível[63].

Assim, algoritmos de IA utilizam extensivas bases de dados *(input)* de forma a reconhecer padrões que não foram previamente estabelecidos pelos programadores, a fim de obter determinados resultados *(output)* para problemas específicos.

[62] Neste texto especificamente os termos inteligência artificial, algoritmo e software são usados de forma intercambiável.

[63] KAPLAN, Andreas e HAENLEIN, Michael. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, Vol. 62, Edição 1, janeiro-fevereiro de 2019. p. 17. Disponível em: <https://bit.ly/2RLaaHG>. Acessado em: 07/02/2019.

Atualmente, não existem regulações claras no Brasil sobre o uso de algoritmos de IA para diagnósticos na saúde. Entretanto, em 2022 a Agência Nacional de Vigilância Sanitária (ANVISA) estabeleceu requisitos específicos para a regularização de softwares como dispositivos médicos (Software as a Medical Device - SaMD), por meio das Resoluções da Diretoria Colegiada da Anvisa nº 657/2022 e 751/2022, que, apesar de não fazerem referência expressa a sistemas IA, é possível fazer uma analogia dos softwares que utilizam sistemas e ferramentas de IA para propósitos médicos à definição de SaMD.

Portanto, a *startup* do caso relatado deve, em primeiro lugar, aderir às normas aplicáveis aos dispositivos médicos, o que engloba regulamentos para classificação de risco, notificação e registro, rotulagem e instruções de uso. Além disso, a depender da classificação da SaMD, empresa é obrigada a fornecer, durante o processo de regularização, informações relacionadas à (i) arquitetura de software; (ii) controles de cibersegurança implementados; (iii) estratégias de gerenciamento de risco adotadas; e (iv) a descrição dos algoritmos utilizada para funcionamento do dispositivo[64]. A falta dessas informações pode resultar na não aprovação ou no indeferimento do pedido de regularização do dispositivo junto à autoridade regulatória.

De toda a forma, a específica regulamentação de algoritmos tem ganhado destaque nas preocupações legais globais, sendo atualmente objeto de desenvolvimento em vários países e organizações internacionais. As leis vinculativas, em sua maioria, estão concentradas no âmbito da proteção de dados, como a LGPD, com uma escassez de normas específicas para o uso de algoritmos em diagnósticos de saúde.

[64] Brasil. Agência Nacional de Vigilância Sanitária. Resolução da Diretoria Colegiada - RDC nº 657, de 2022. Dispõe sobre a regularização de software como dispositivo médico (Software as a Medical Device - SaMD). Art. 12. Disponível em: https://antigo.anvisa.gov.br/documents/10181/5141677/RDC_657_2022_.pdf/f1c32f0e-21c7-415b-8b5d-06f-4c539bbc3. Acesso em: 05 de março de 2024.

Somada às leis vinculativas, a abordagem regulatória encontra força na adoção de códigos de conduta e diretrizes não vinculativas *(soft law)* como parte de um processo em constante evolução para enfrentar os desafios éticos e legais relacionados à implementação de algoritmos na área da saúde. Vale ressaltar a iniciativa da Organização Mundial da Saúde (OMS)[65], que, por meio de princípios éticos gerais para o desenvolvimento de IA e a integração de elementos da bioética, busca alinhar-se à regulamentação atual em saúde, proporcionado orientações para o uso responsável da IA na área da saúde[66].

Nesse sentido, um ponto de atenção para o desenvolvimento dos sistemas de IA pela startup estará relacionado a efetivação da transparência algorítmica e explicabilidade das decisões tomadas pelos algoritmos empregados no software. Isso porque a LGPD prevê o direito do titular de requisitar informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. Este direito tem relevância no desenvolvimento de IA, pois estabelece a necessidade de que a lógica decisória utilizada pelo algoritmo seja construída de forma a ser inteligível ou compreensível para desenvolvedores, usuários e reguladores.

Em resumo, o direito à explicação garante que todas as pessoas tenham o direito de entender como as decisões baseadas em IA que afetam suas vidas são tomadas. Contudo, ainda não se sabe ao certo quais serão os limites do que seria uma explicação adequada sobre a lógica decisória, principalmente quando se considera que alguns algoritmos de IA, devido a sua complexidade, são conhecidos como sistemas de "caixa-preta". Termo que se refere a uma característica técnica relativa à incapacidade dos programadores em explicarem como uma IA chegou a determinado resultado[67].
Este problema afeta diretamente os limites de um possível direito a explicação e como ele será efetivado na prática.

[65] World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva (CH): WHO; 2021. Disponível em: https://www.who.int/publications/i/item/9789240029200. Acesso em: 05 mar. 2024.

[66] DOURADO, D. A.; AITH, F. M. A. A regulação da inteligência artificial na saúde no Brasil começa com a Lei Geral de Proteção de Dados Pessoais. Revista de Saúde Pública, v. 56, p. 80, 2022. Disponível em: https://www.scielo.br/j/rsp/a/k38jGvJdbQSYN4MpzGZpfXw/?format=pdf&lang=pt. Acesso em: 05 mar. 2024.

[67] KNIGHT, Will. The Dark Secret at the Heart of AI: No one really knows how the most advanced algorithms do what they do. That could be a problem. MIT Technology Review. Edição de Maio/Junho 2017. Disponível em: <https://bit.ly/2otrSjZ>. Acessado em: 07/02/2019

O direito à explicação é fundamental no tratamento de dados pessoais de saúde, pois possibilita que os pacientes compreendam o processo de tomada de decisões automatizadas que impactam seus cuidados. Isso é essencial para permitir a identificação de erros pelos avaliadores do sistema e facilitar a supervisão eficaz por parte dos reguladores governamentais. Além disso, a possibilidade de auditar a tecnologia de IA, mesmo em casos de falhas, é necessária para assegurar a responsabilidade e a confiança no uso desses sistemas no contexto da saúde.

Os titulares afetados por IAs também possuem o direito de requisitar uma revisão das decisões baseadas unicamente no tratamento automatizado de seus dados[68]. Entretanto, ainda não está definido o escopo do que significaria a palavra "unicamente". Assim, por exemplo, caso o diagnóstico final seja dado pelo médico não está claro se esta participação humana descaracterizaria o termo "decisões tomadas unicamente com base em tratamento automatizado".

É provável que esse termo não seja interpretado de forma a considerar qualquer intervenção humana, mas apenas aquelas que tenham a capacidade de alterar a decisão automatizada[69], como no exemplo do médico.

Outro ponto a ser destacado é a necessidade dos desenvolvedores de IA de se respaldarem em uma das bases legais da LGPD para utilização de dados pessoais para o treinamento de algoritmos. Assim, por exemplo, se um plano de saúde desenvolver um projeto para criar uma IA de diagnóstico de câncer, treinada a partir de uma base de dados de tomografias de seus pacientes, seria necessário fundamentar esse tratamento em uma base legal. Outra possibilidade seria que esses dados fossem anonimizados de forma a deixarem de ser considerados dados pessoais pela LGPD, o que permitiria uma maior liberdade na sua utilização.

[68] D  BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 20º.

[69] UNIÃO EUROPEIA. Working Party 29. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679. 2017. p. 21. Disponível em: <https://bit.ly/2R4lejM>. Acessado em: 08/02/2019.

← *voltar ao sumário*

**Introdução**

1. Dado pessoal, dado sensível e dado de saúde

2. Como deve ser o consentimento para o uso de dado de saúde?

3. Anonimização e pseudonimização

4. Hipóteses legais que permitem o compartilhamento de dados de saúde

5. Direitos dos titulares dos dados

6. Dados de saúde de funcionários

7. Responsabilização dos agentes por descumprimento da Lei Geral de Proteção de Dados

8. Melhores práticas de proteção de dados para dados de saúde

9. Relatórios de Impacto à Proteção de Dados na área da saúde

10. Algoritmos de inteligência artificial e a proteção de dados pessoais

**Conclusão**

# Conclusão

As práticas do setor de área da saúde requerem constantes preocupações com a Lei Geral de Proteção de Dados. Desde o conceito de dados sensíveis, inferências, bases legais restritas que legitimam o tratamento, até mesmo limitações ao compartilhamento para fins de obtenção de vantagem econômica e o intenso uso de algoritmos de inteligência artificial para fins de medicina preventiva e diagnóstica. É necessário que os entes regulados entendam as obrigações aplicáveis às suas práticas e as medidas de adequação que devem ser implementadas, seja por meio de práticas de educação, conscientização, e uso de metodologias, como relatórios de impacto à proteção de dados, para se adequarem corretamente, visando a conformidade com a norma e a mitigação de riscos aos direitos e liberdades dos titulares dos dados.

b/luz

baptistaluz.com.br