Dados de Saúde e a Lei Geral de Proteção de Dados:

Estudo de casos

BAPTISTA LUZ
ADVOGADOS

Autores

_ Adriane Loureiro Novaes

_ Camila de Vito

_ Fernando Bousso

_ Gabriela Moribe

_ Luiza Balthazar

_ Matheus Botsman Kasputis

_ Odélio Porto Júnior

_ Rafael Pessoa

_ Renato Leite Monteiro

Sumário

Introdução _03

1 Dado Pessoal, Dado Sensível e Dado de Saúde: como legitimar o tratamento desses dados? _04

2 Como deve ser o consentimento para utilizar Dados de Saúde? _09

3 Anonimização e Pseudonimização _012

4 Hipóteses legais que permitem o compartilhamento de Dados de Saúde _016

5 Direitos dos Titulares dos Dados: definição e limitações legais _019

6 Dados de Saúde de funcionários _022

7 Responsabilização por descumprimento da Lei Geral de Proteção de Dados _026

8 Melhores práticas de proteção de dados para Dados de Saúde _030

9 Relatórios de Impacto à Proteção de Dados em empresas do setor de saúde - intersecção entre GDPR e LGPD _034

10 Algoritmos de Inteligência Artificial e a Proteção de Dados Pessoais _038

Conclusão _042

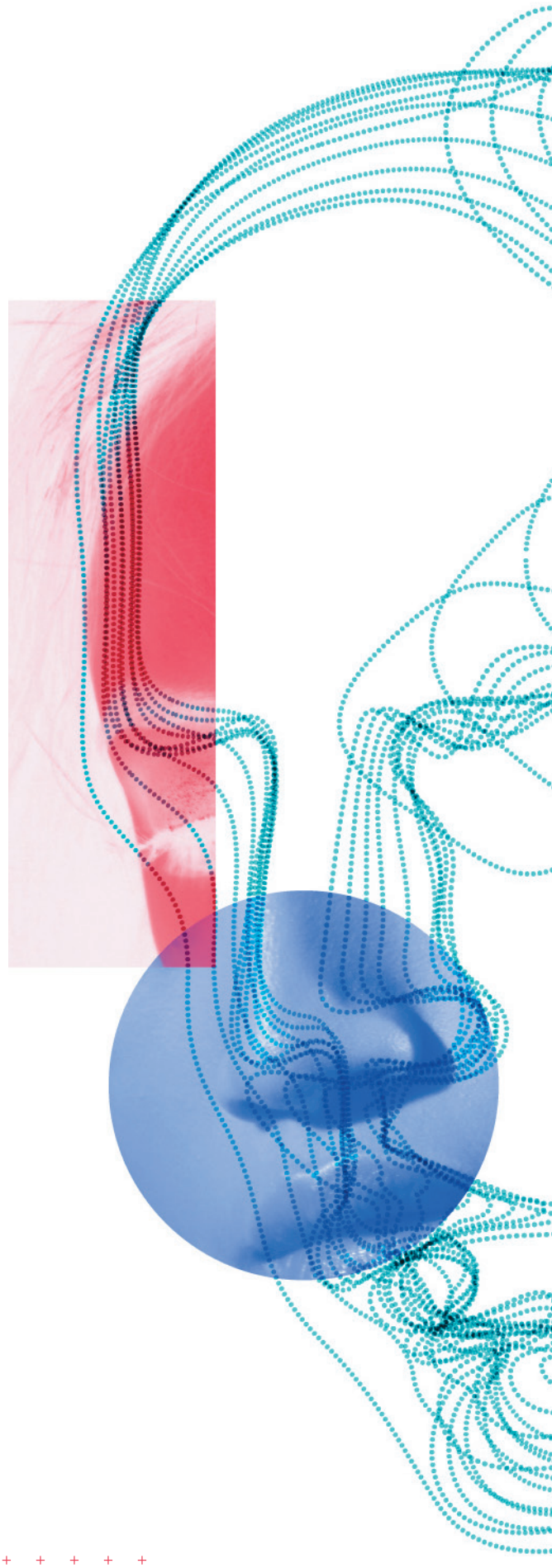
Glossário _043

_Introdução

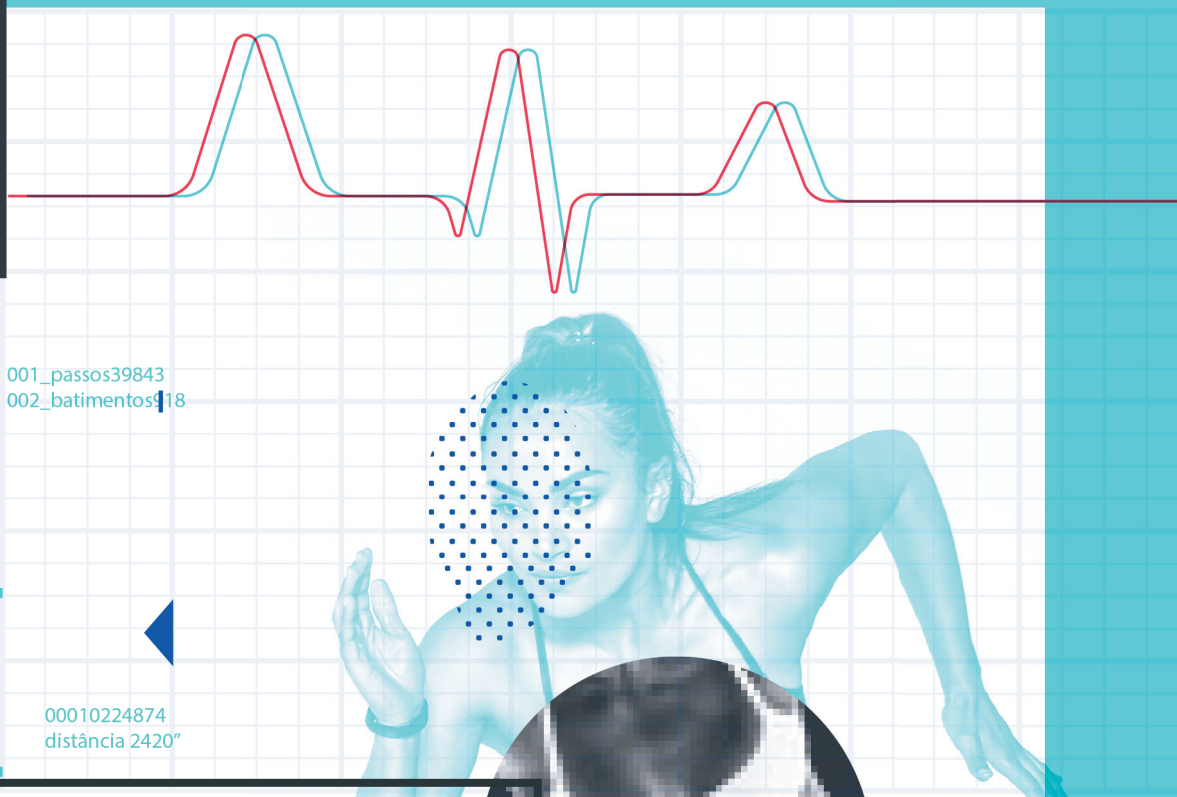
Apesar da sensibilidade inerente dos dados de saúde, o respectivo setor atualmente carece de regras claras de proteção de dados pessoais. Atualmente, as normas existentes se limitam, com algumas exceções, a delinear regras gerais sobre o compartilhamento de dados entre setor público e privado, consentimento para a coleta desses dados e armazenamento de prontuário médico.

Nesse sentido, a Lei Geral de Proteção de Dados ("LGPD") impactará (e muito) o setor de saúde. Áreas como medicina de precisão e diagnóstica, e-Health e telemedicina vão ser diretamente impactadas pela LGPD, mas devem enxergar um projeto de conformidade com a nova lei não como um ônus, mas 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 de como o setor de saúde será afetado pela LGPD, por meio de estudo de casos hipotéticos, mas com possibilidade de efetiva aplicação prática.



1



Dado Pessoal, Dado Sensível e Dado de Saúde: *como legitimar o tratamento desses dados?*

Uma determinada empresa 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 Lei Geral de Proteção de Dados ("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 Lei Geral de Proteção de Dados ("LGPD", Lei nº 13.709/18), estes conceitos podem ser definidos da seguinte maneira:

"Dado Pessoal"[1]: é a informação relacionada a pessoa natural identificada ou identificável. PPor exemplo, encontram-se nessa categoria dados como nome, número de telefone, e-mail, identificadores únicos eletrônicos (como IP, cookies, beacons, etc), entre outros. Ainda, esse conceito inclui dados que isolada ou conjuntamente, em um determinado contexto, possam permitir a identificação de alguém. O conceito engloba, também, dados que podem sujeitar uma pessoa natural individualizada a uma determinada atividade, comportamento, ou ação (prática conhecida como *"singling out"*), tornando por vezes desnecessário saber efetivamente quem essa pessoa é (saber se trata-se de Maria ou João), desde que haja um identificar único atrelado a este indivíduo.

1_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso II.

“Dado Sensível”[2]: é um conceito específico dentro da categoria de dado pessoal.São os dados que, por sua sensibilidade, podem ser utilizados para fins discriminatórios, exigindo, por isso, padrões mais rigorosos para o seu tratamento. São eles: 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 engloba, ainda, dados pessoais que, num primeiro momento, podem não parecer sensíveis, como a localização de um indivíduo (p. ex. informações de geolocalização de uma pessoa que está semanalmente em uma determinada igreja ou espaço de culto) mas que, devido ao contexto da sua coleta, podem permitir inferir dados sensíveis (neste caso, a sua convicção religiosa)[3].

“Dado de Saúde”[4]: conforme exposto acima, os dados de saúde estão dentro da categoria de dados sensíveis, incluindo os dados referentes à saúde ou à vida sexual, os dado genéticos e biométricos. Por exemplo: tipo sanguíneo, se é doador de órgãos, se é portador de determinada doença, frequência cardíaca, etc. Esse conceito engloba, também, dados pessoais que, num primeiro momento, podem não parecer ser de saúde, mas que, dentro de um contexto, podem permitir inferir dados de saúde, como a frequência de corridas de um determinado indivíduo.

“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 a depender da categoria do dado e a finalidade do tratamento. Cumpre salientar que as bases legais são distintas a depender da categoria do Dado Pessoal. A LGPD traz 10 hipóteses para o tratamento dos dados pessoais[6] em geral e 8 hipóteses para o tratamento de dados sensíveis[7], caso dos dados de saúde. Para a categoria geral de dados pessoais, o legislador optou por conferir às Bases Legais o mesmo peso, isto é, o consentimento valeria tanto quanto a base legal da tutela da saúde, do legítimo interesse etc, 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. Já para os dados sensíveis, o legislador optou por dar uma importância maior ao consentimento, sendo as outras bases podem fundamentar um tratamento em caráter excepcional, somente para os casos em que a coleta dos dados for

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.

4_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º. Inciso II.

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.

indispensável[8] para atingir o objetivo da base legal em comento, como proteção a vida. Enumeramos as bases legais no quadro abaixo:

Dado Pessoal (hipótese geral)	**Dado Sensível** (específica)
1) consentimento; **2)** obrigação legal; **3)** políticas públicas; **4)** estudos por órgão de pesquisa; **5)** execução de contrato; **6)** exercício regular de direito em processo **7)** proteção da vida ou da incolumidade física; **8)** tutela da saúde; **9)** legítimo interesse; e **10)** proteção do crédito.	**1)** consentimento; **2)** obrigação legal; **3)** políticas públicas; **4)** estudos por órgão de pesquisa; **5)** exercício regular de direito em processo; **6)** proteção da vida ou da incolumidade física; **7)** tutela da saúde por profissionais da saúde; e **8)** garantia de prevenção à fraude e à segurança do titular.

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."

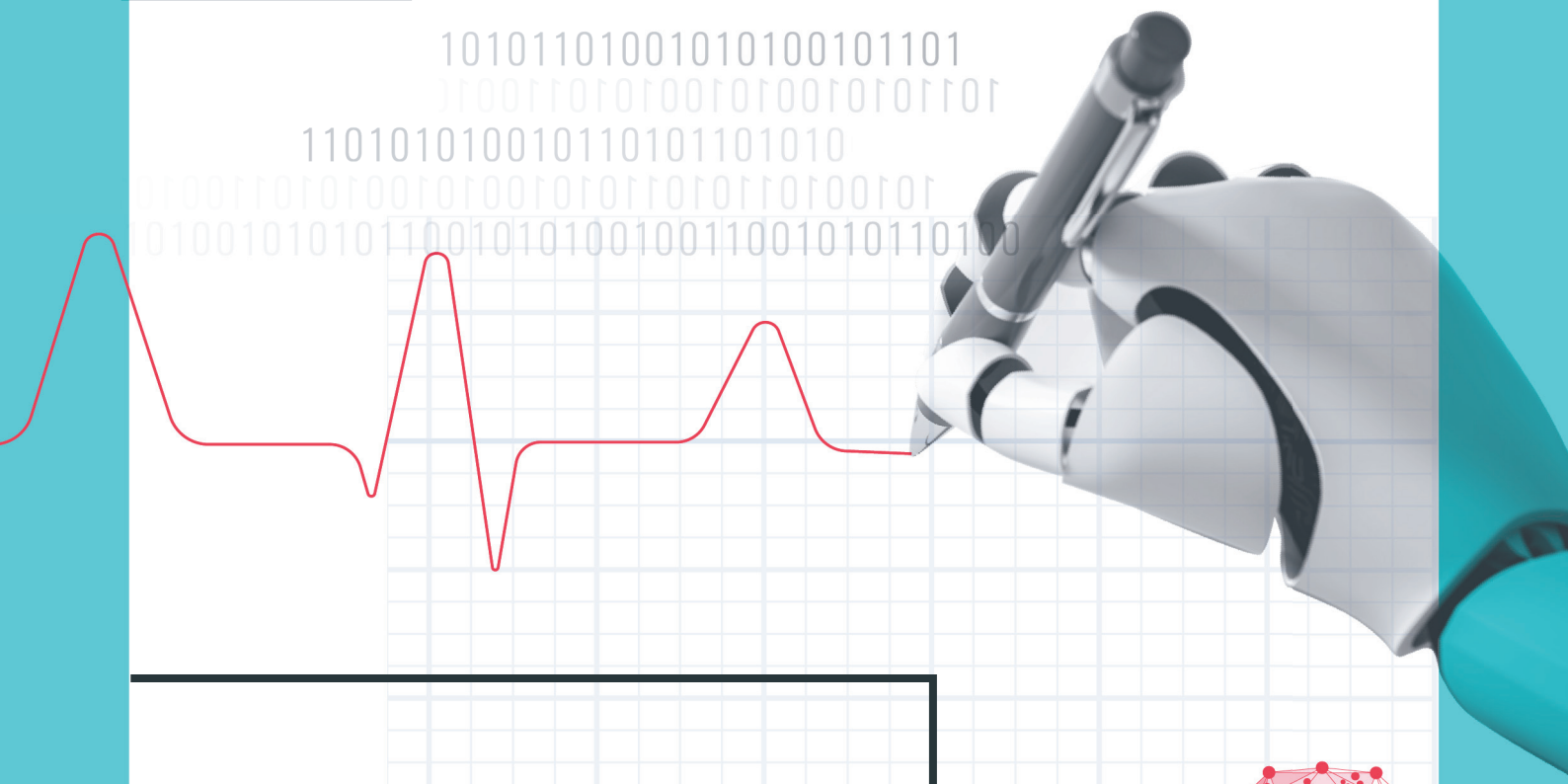
Em outras palavras, a LGPD estabeleceu que o consentimento específico e destacado do titular, para finalidades específicas, deve sempre ser buscado para o tratamento de dados sensíveis. Não se trataria, na estrutura escolhida pelo legislador, de uma faculdade, uma opção, mas uma regra, e as demais bases legais deveriam fundamentar o tratamento de dados sensíveis, inclusive os de saúde, somente quando forem indispensáveis para: a) o cumprimento de uma obrigação legal ou regulatória pelo controlador; b) o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) a proteção da vida ou da incolumidade física do titular ou de terceiro; f) a tutela da saúde, em procedimento que precisa ser realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Essa estrutura normativa mais restritiva privilegia, portanto, a participação ativa do titular do dado pessoal sensível por meio do consentimento, autorizando o tratamento do seu dado, em detrimento às demais hipóteses, que são balanceadas com outras obrigações, como de transparência e informação. 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 controlador e, até mesmo, um terceiro, como a sociedade. Um exemplo desse exercício seria o tratamento de dados de saúde para execução de políticas públicas. Neste caso, sim, poderia ser possível, em tese, obter o consentimento de todos os titulares. Todavia, obter o consentimento de todos os titulares que podem ser atingidos por determinada política poderia trazer ônus e custos superiores ao benefício geral de referida política. Desta forma, seria possível se valer da base de políticas públicas para legitimar o tratamento. A mesma lógica pode ser aplicada às demais bases legais, com as devidas salvaguardas e peculiaridades de cada caso.

No caso em tela, é possível afirmar que o Aplicativo trata tanto dados pessoais quanto Dados de Saúde. Inevitavelmente, informações como peso, altura e batimentos cardíacos podem ser classificadas como dados sensíveis. Já as outras informações como marcador de passos e distância percorrida, que em um primeiro momento parecem ser apenas dados pessoais, podem ser classificados como dados de saúde se a inferência gerada a partir desses dados for uma informação de saúde, por exemplo: se a partir do marcador de passos diários for possível concluir que se trata de um usuário sedentário.

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

2



Como deve ser o consentimento para utilizar Dados de Saúde?

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 nova Lei Geral de Proteção de Dados brasileira.

O consentimento para o tratamento de Dados de saúde, classificados como dados sensíveis[9] pela Lei Geral de Proteção de Dados (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. Nesse sentido, uma das principais dúvidas das empresas e profissionais de saúde é a forma como esse consentimento deve ser obtido dos pacientes (que são os titulares dos dados), principalmente porque ele pode ser obtido na maioria dos casos onde há o tratamento de dados saúde. A preocupação com a forma é importante, pois a lei busca proteger e empoderar o titular (consequência direta do princípio da autodeterminação informativa), para que ele tenha um mínimo de controle sobre se, como e quando seus dados serão utilizados, ainda mais por se tratar de dados críticos que podem ser usados tanto de forma positiva quanto abusiva.

A LGPD define como dever ser obtido o consentimento para dados sensíveis e de saúde por meio de uma série de requisitos que devem ser postos em prática pelo responsável pelo tratamento: **(i) informado**; **(ii) livre**; **(iii) finalidades determinadas**; **e (iv) específico**. Esses termos não são meros sinônimos, possuem significados distintos, que afetam a qualidade do consentimento obtido. Desse modo, explicamos a seguir o significado de cada um:[10]

I. **Informado:** exige que o titular seja informado, uso e compartilhamento de seus dados pessoais de forma clara e de fácil entendimento;

II. **Livre:** seria um ato do titular que não foi realizado por meio de coação física moral, psicológico ou artifício que o induza. Trata-se de uma efetiva escolha da sua parte, com a opção de simplesmente não consentir, mesmo que isso tenha um impacto na sua vida, o que deve ser previamente informado. O tratamento de dados de saúde de empregados por empregadores é um exemplo interessante sobre a dificuldade de se obter um consentimento livre, pois a relação de hipossuficiência entre o trabalhador e o empregador pode retirar a sua liberdade em optar ou não autorizar o tratamento dos seus dados, maculando o consentimento;

III. **Finalidades Determinadas:** refere-se à necessidade de demonstração clara sobre quais serão as finalidades do tratamento dos dados, não sendo permitido autorizações genéricas nem usos que fogem ao contexto do tratamento. Um exame médico, por exemplo, poderia ter a finalidade tanto de fornecer um diagnóstico para o paciente como para fins de uso das informações para desenvolvimento de novos medicamentos, entre inúmeros outros uso;

IV. **Específico:** esta característica busca enfatizar a necessidade de uma confirmação assertiva da vontade do titular de autorizar o tratamento de seus dados, exigindo sua participação ativa, que confirme que ele entende que seu dado será tratado para uma finalidade específica. Este adjetivo, por exemplo, limita autorizações que englobem, de uma vez só, muitas finalidades, principalmente as que podem ter um impacto no indivíduo.

Como a LGPD foi fortemente influenciada pela regulação da União Europeia é interessante observar como a ideia de "consentimento"

9_Tema 1 deste guia.

10_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.

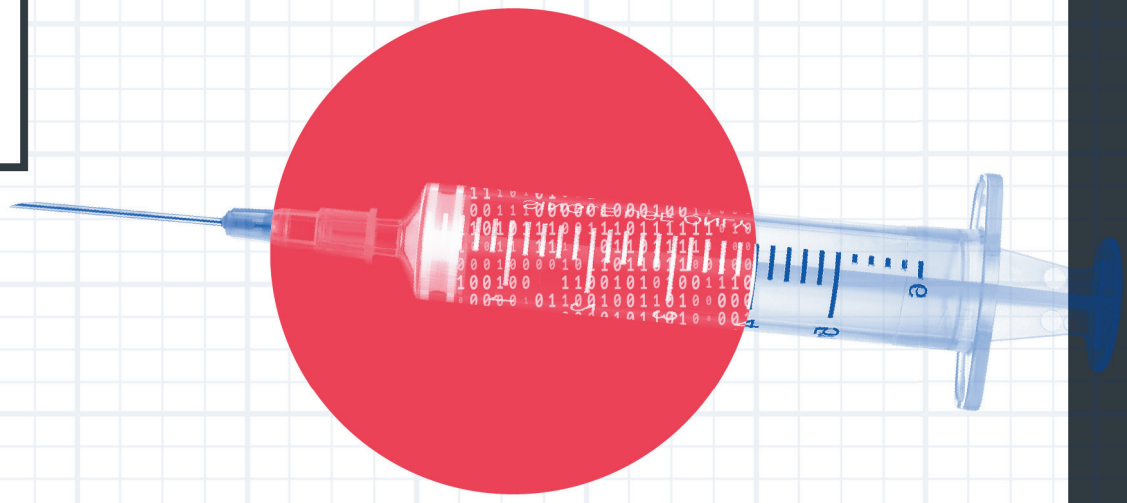
adequado tem sido discutida pelos países do bloco. Atualmente, tem sido dada enfase à ideia de "consentimento ativo", que sugere a impossibilidade de obtenção do consentimento de forma implícita, pela mera inação do titular dos dados em não se opor ao tratamento, ou por seu uso reiterado de determinado serviço.[11] Assim, um consentimento ativo busca incentivar o engajamento direto do titular, bem como o fornecimento de informações claras que embasem a 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. Ademais, caso haja alteração das finalidades de tratamento, deve-se informar o titular previamente para que seja coletado um novo consentimento. E, por fim, deve ser garantido à pessoa, de forma facilitada, o direito de revogação de seu consentimento e de exclusão de seus dados pessoais, a não ser que o controlador consiga fundamentar a continuidade do tratamento por uma das outras hipóteses legais da LGPD, o que não significa que seria possível fundamentar o tratamento concomitantemente em mais de uma base legal.

Ao se analisar o exemplo utilizado, verifica-se que as finalidades (i) "desenvolvimento de nossas atividades" e (ii) "promoção do seu bem-estar" podem acabar por serem qualificadas como 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". Assim, as finalidades se tornam mais claras, específicas, determinadas. Em relação à linguagem do documento, seria de bom tom acrescentar um infográfico que traduzisse a linguagem jurídica do Termo, garantido assim que o consentimento seja devidamente informado. A fim de qualificar o consentimento como livre, recomenda-se atentar para o treinamento dos funcionários para evitar qualquer tipo de coação ou imposição, pois a simples exigência de assinatura sem as devidas explicações, sem a possibilidade de discordar do tratamento, ou a ausência de esclarecimento de dúvidas podem violar a livre manifestação de vontade. E, por fim, a obtenção de um consentimento específico pode ser alcançado com a assinatura do titular, ou o seu "ok" de forma separada, após as qualificações acima terem sido devidamente atendidas, sendo importante registrar todo esse caminho por questões de accountability, uma vez que cabe ao controlador comprovar que obteve de forma adequada o consentimento.

11_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.

3



Anonimização e Pseudonimização

Uma empresa tradicional do setor de saúde deseja utilizar a base de dados de exames clínicos que já possui, para compartilhar com a indústria farmacêutica com o objetivo de criar 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 esta. 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 essa desenvolva novos medicamentos e tratamentos de saúde.

Em respeito aos princípios da finalidade e da adequação, descritos na Lei Geral de Proteção de Dados ("LGPD"), todo e qualquer processamento 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[12], o processamento de dados pessoais deve ser feito para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedada a possibilidade de processamento posterior de forma incompatível com o que foi informado ao titular. Já o princípio da adequação[13] dispõe que o processamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular e de acordo com o contexto do processamento.

Além disso, a LGPD restringe o compartilhamento de dados de saúde com objetivo de obter vantagem econômica, caso esse compartilhamento não seja para (i) a prestação de serviços de saúde; (ii) a prestação de assistência farmacêutica; (iii) assistência à saúde, incluindo serviços auxiliares de diagnose e terapia; (iv) a portabilidade, a pedido do titular; e (v) permitir as transações financeiras e administrativas relacionadas ao serviços elencados anteriormente. [14] 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 do paciente realizar os exames clínicos.[15]

Ainda, de acordo com a LGPD, não está claro se mesmo com o consentimento específico[16] do titular dos dados de saúde, seria possível autorizar o compartilhamento de seus dados com outra empresa (na qualidade de controladora, no caso em questão), com o objetivo de obtenção de vantagem econômica, a exceção dos casos listados acima. Esta leitura da LGPD, portanto, determina que o compartilhamento com fins de obtenção de vantagem econômica somente poderia acontecer nos casos retro elencados, e outras situações não poderiam se valer do consentimento para serem viabilizadas, numa clara aplicação do princípio da precaução.

Contudo, para viabilizar o negócio da empresa e o desenvolvimento 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, que está inserido na seção específica de dados pessoais sensíveis, estabelece expressamente que dados anonimizados não serão considerados dados pessoais para os fins da referida Lei, salvo quando o processo de anonimização puder ser revertido com esforços razoáveis.

Para determinação do que é razoável, a LGPD dispõe que deve ser levado em consideração

12_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso I.

13_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso II.

14_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º, §4º.

15_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 15º, inciso I.

16_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 7º, §5º.

fatores objetivos como (i) o custo dispendido para a realização do processo de anonimização; e (ii) o tempo necessário para reverter tal processo; ponderando as tecnologias disponíveis no momento.[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]

A impossibilidade de identificação do titular retira os dados anônimos 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; e (iii) conceder os direitos de informação, de acesso, retificação e eliminação dos titulares; entre outras vantagens.

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 especificas 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 re-identificação destas.

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 à 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

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.

19_ https://www.ema.europa.eu/en/human-regulatory/marketing-authorisation/clinical-data-publication

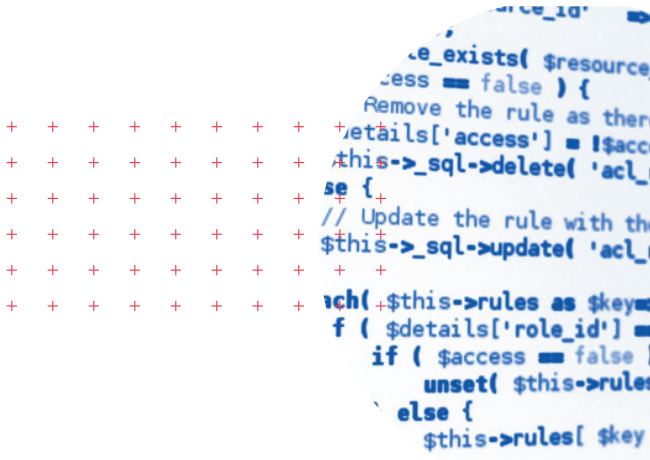
20_ https://www.ema.europa.eu/documents/regulatory-procedural-guideline/external-guidance-implementation-european-medicines-agency-policy-publication-clinical-data_en-3.pdf

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. Ainda, de acordo com a LGPD, dados pseudonimizados só podem ser utilizados na realização de pesquisas de saúde pública[21] feitas por órgãos de pesquisa.[22] Uma clínica ou uma empresa da indústria farmacêutica provavelmente não seriam classificadas como órgãos de pesquisa, pelo conceito da LGPD, por terem fins lucrativos.

Cabe à Autoridade Nacional de Proteção de Dados ("ANPD") se posicionar e dispor sobre padrões e técnicas utilizados em processos de anonimização, bem como realizar verificações acerca de sua segurança[23]. Até que isso aconteça, todavia, as empresas podem se orientar por metodologias sugeridas por autoridades de proteção de dados estrangeiras, principalmente as da União Europeia, uma vez que a LGPD foi fortemente influenciada pela GDPR e as opiniões de seus entes consultivos, como o *Working Party 29* e o *European Data Protection Board*. Já houve posicionamento, por exemplo, afirmando que dados pessoais podem eventualmente não ser efetivamente anonimizados de acordo com a segurança e o risco do processo de anonimização adotado. [24]

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.



21_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 13.

22_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5, XVIII - órgão de pesquisa: 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.

23_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 12º, §3º.

24_ Opinion 05/2014 on Anonymisation Techniques. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em 06.02.2019.

4

Hipóteses legais que permitem o compartilhamento de dados de saúde

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) à 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 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, importante ter em mente que 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[25], o processamento de dados pessoais deve ser feito para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedada a possibilidade de processamento posterior de forma incompatível com o que foi informado ao titular. Já o princípio da adequação[26] dispõe que o processamento dos dados pessoais deve ser compatível com as finalidades informadas ao titular e de acordo com o contexto do processamento.

Além disso, importante observar que possivelmente tais dados serão interpretados como dados sensíveis, na medida em que permitem inferir dados referentes à 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 e realizar os pagamentos e entregas, estejam sendo coletados para a melhoria dos serviços e da experiência do usuário na plataforma. Sendo assim, tratamentos secundários dos dados, quais sejam, a comercialização destes e avaliação dos riscos dos titulares por empresas de planos e seguros de saúde, pode não ser considerado compatíveis com os fins para os quais os dados foram originalmente coletados.

Ainda, a LGPD autoriza o compartilhamento de dados de saúde com objetivo de obter vantagem econômica somente em determinadas situações. Com as alterações no texto legal trazidas pela Medida Provisória nº 869/2018, as hipóteses de compartilhamento aumentaram. Assim, é permitido realizar o compartilhamento de dados de saúde entre controladores, com objetivo de obter vantagem econômica, nas hipóteses relacionadas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluindo serviços auxiliares de diagnose e terapia. Também será permitido o compartilhamento de dados de saúde para realizar a portabilidade dos dados quando solicitada pelo titular, e para permitir as transações financeiras e administrativas relacionadas ao serviços elencados anteriormente. [27]

Ademais, não é permitido que as operadores de planos privados de assistência à saúde realizem tratamento de dados de saúde (p. ex. processamento, compartilhamento,

25_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso I.

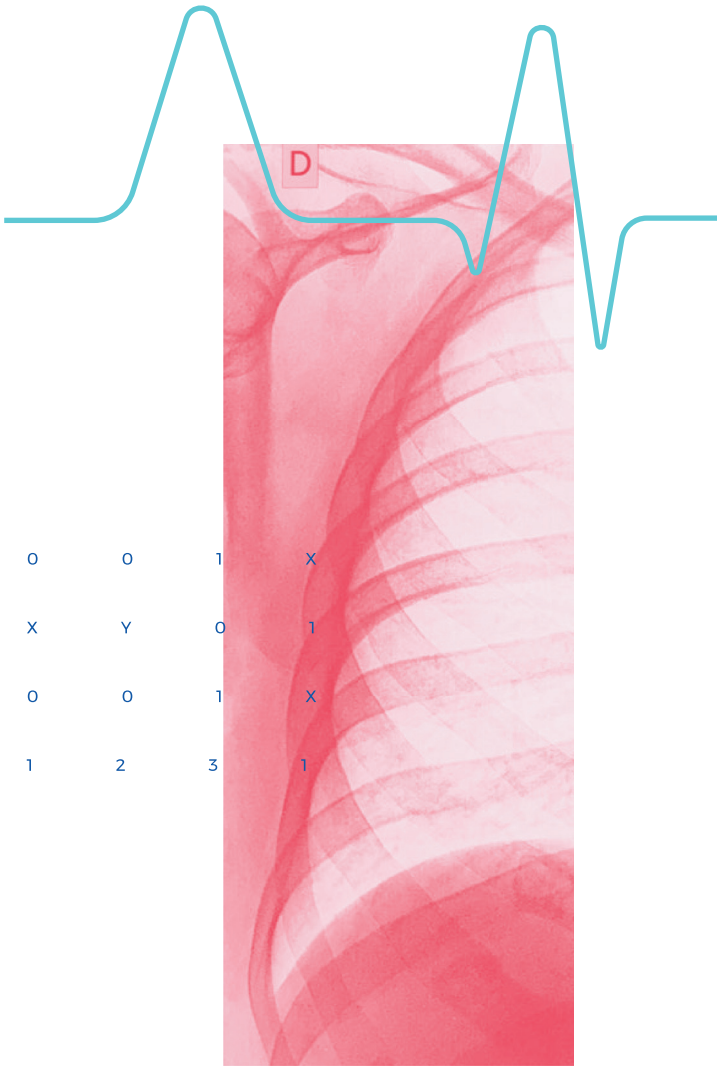
26_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso II.

27_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º, §4º.

classificação, etc[28]) (i) realizar seleção de riscos na contratação de qualquer modalidade, e na (ii) contratação e exclusão de beneficiários.[29]

Entretanto, os termos utilizados para descrever as hipóteses de compartilhamento podem ser considerados bastante amplos. Nesse sentido, portanto, é possível que Autoridade Nacional de Proteção de Dados Pessoais possa vir a regular de forma mais específica determinados setores do ecossistema de saúde privada.[30] 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 sáude? É igualmente difícil obter parâmetros e/ou entendimentos de autoridades de proteção de dados estrangeiras, pois esse dispositivo existe apenas na legislação brasileira. A ANPD terá um papel primordial na elucubração de tais dúvidas, que antes de serem dirimidas devem ser analisadas por meio de exercícios de colaboração entre diferentes órgãos reguladores, como ANS, representantes da iniciativa privada e entidades do terceiro setor.

Por fim, em relação ao caso fictício posto como exemplo, 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. Possivelmente, haveria uma violação aos princípios gerais como da finalidade e adequação. Ainda, tal caso dificilmente seria interpretado como uma das hipóteses que autorizam o compartilhamento de dados de saúde com fins de obtenção de vantagem econômica. Todavia, potencialmente seria possível se valer de tais dados de forma anonimizada, visando entender os hábitos gerais de um determinado grupo, desde que os dados agrupados não sejam atribuídos a indivíduos identificados.

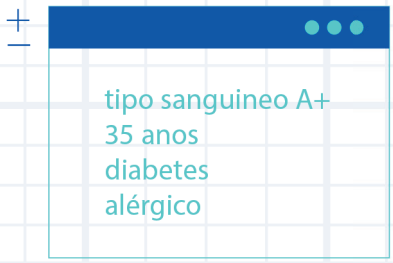


28_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, X.

29_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º, §5º.

30_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11, § 3º.

5



Direitos dos Titulares dos Dados: *definição e limitações legais*

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, que seus dados no antigo fossem excluídos. Pergunta-se, o hospital pode manter os dados?

O caso apresentado acima envolve a questão dos **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[31]:

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) portabilidade 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;

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[32], sendo permitida a manutenção destes para atender às seguintes finalidades:

1) cumprimento de obrigação legal ou regulatória pelo controlador;

2) estudo por órgão de pesquisa[33], 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;

4) uso exclusivo do controlador, vedado seu

31_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, I a IX e Artigo 20.

32_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 16, I a III.

33_"Órgão de Pesquisa" é definido na 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".*

acesso por terceiro, e desde que anonimizados os dados.

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

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[34], não havendo obrigação de transferência em relação aos dados eventualmente anonimizados[35]. 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;

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[36]. Outros dados, que não estão em prontuário médico também devem ser excluídos, caso não exista uma hipótese, uma base legal, que permita sua manutenção.

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 novos padrões de interoperabilidade e formas de cumprir com os pedidos de requisição de direitos.

34_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 40.

35_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 18, § 7º.

36_BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Artigo 6º.

6

Dados de saúde de funcionários

Uma empresa, que atua no setor de Engenharia e Construção pretende realizar o controle e monitoramento dos smartphones corporativos utilizados por seus funcionários. Além de coletar dados de geolocalização, a empresa pretende coletar dados que permitem aferir se o funcionário pratica exercícios físicos ou não, com o objetivo de oferecer plano de saúde empresarial coletivo a seus colaboradores adequado aos seus hábitos. Para tanto, a empresa se 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 coorporativo oferecido a seus funcionários, coletar dados que permitam aferir se o funcionário pratica exercícios físicos ou não, 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[37], ou permita inferir tal estado de forma significativa. 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[38].

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, estabelece obrigações específicas em relação aos dados pessoais de empregados. 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 contém 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, com 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, estabelecendo 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.

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 destes, 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 (e não para aferir a prática de exercícios físicos ou não pelo funcionário, como pretendido pela empresa), 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

37_Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records, 15 February 2007.

38_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, inciso II.

restringir as atividades laborais, sendo vedado 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.

Além disso, com a **Lei Geral de Proteção de Dados no Brasil** ("LGPD"), algumas **regras adicionais** deverão ser observadas pelas companhias quando forem processados os dados pessoais de seus empregados. De acordo com a LGPD, para coletar, processar, armazenar e divulgar um dado pessoal de um empregado, o empregador deverá (i) observar os **princípios** trazidos pela LGPD[39]; (ii) ter uma **base legal** que justifique o processamento de dados pessoais e/ou sensíveis de seus empregados[40]; e (iii) cumprir com os **direitos dos titulares de dados**[41]; dentre outras obrigações.

Como dito anteriormente, os dados pretendidos 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 possibilitam o tratamento de dados sensíveis de acordo com a LGPD é o **consentimento** do titular (no caso, o funcionário), que deve ser **livre, informado e inequívoco**, bem como realizado de forma **específica e destacada**[42]. 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 processamento dos seus dados e sem que haja penalidade caso o funcionário se oponha ao tratamento.

Dado o desequilíbrio existente na relação empregador/empregado, é pouco provável que o funcionário possa negar seu consentimento ao empregador para o processamento de seus dados pessoais sem que o funcionário experimente o medo ou o risco de efeitos prejudiciais causados pela recusa. É improvável que um funcionário possa responder livremente a uma solicitação de consentimento vinda de seu empregador para, por exemplo, ativar sistemas de monitoramento, como observação de câmeras em um local de trabalho ou em seu smartphone, ou preencher formulários de avaliação, sem sentir qualquer pressão.

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.

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 do smartphone corporativo, 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

39_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 6º, incisos I a X.

40_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigos 7º e 11º.

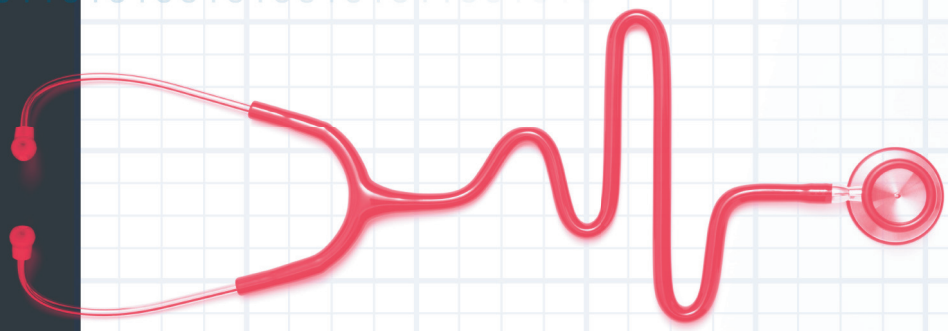
41_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 9º.

42_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º.

(ii) tal prática desafia o princípio da necessidade, podendo ser considerado uma coleta excessiva, além de possivelmente não possuir uma base legal segura que legitime o processamento de tais dados, pois o consentimento provavelmente não seria considerado livre.

Todavia, isso não deve impedir que sejam ofertados benefícios aos colaboradores, de forma individual ou coletiva. Por exemplo, a possibilidade de exames periódicos, que devem ser totalmente voluntários, e não podem ser utilizados para qualquer outra finalidade se não permitir que o colaborador possa ter um conhecimento sobre o seu estado de saúde, à exceção de quando houver uma obrigação legal ou regulatória na realização de exames para aferir o estado de saúde do colaborador. O empregador, poderia, ainda, se valer dos dados oriundos de exames para fins, por exemplo, de contratação de planos de saúde coletivos mais adequados, sendo recomendável que tais dados, antes da sua análise, sejam efetivamente anonimizados, impossibilitando identificar a quem tais dados originalmente se referiam. As métricas permitiriam inferir o status coletivo da saúde dos colaboradores da empresa, mas não de forma individualizada.

7



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

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, seja no âmbito do direito civil ou mesmo do direito penal. 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 instituições.

As categorias de responsabilização citadas acima podem ocorrer de forma concomitante, não sendo mutuamente excludentes. Assim, por exemplo, se um hospital privado compartilha dados 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[43], ele pode ser sancionado tanto pela ANPD quanto ser processado pelos pacientes, os quais podem buscar indenizações por danos materiais e/ou morais.

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

> "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; e
>
> VI - eliminação dos dados pessoais a que se refere a infração;" [grifo nosso]

No caso de uma possível infração será iniciado um processo administrativo na ANPD, no qual o acusado possui direito à ampla defesa. 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 [...];

43_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11. Parágrafo 4º.

> 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."

Em conjunto com esses parâmetros, a ANPD deverá criar um regulamento próprio que estabeleça os critérios para aplicação das sanções administrativas, o qual deverá ser, inclusive, objeto de consulta pública.

Uma das principais ocorrências que exigirá uma atuação frequente da Autoridade será em casos que envolvam o vazamento de dados por falha na segurança. Como mostra o estudo quantitativo da ong estadunidense *Identity Theft Resource Center*, os EUA têm apresentado um crescimento constante no número de vazamentos de dados, inclusive no setor de saúde:

ITRC MULTI-YEAR DATA BREACH CHART JAN. 1, 2005-DEC. 31, 2018														
# OF TOTAL BREACHES PER INDUSTRY														
INDUSTRY	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Banking/Credit/Financial	20	31	32	79	58	54	31	24	35	38	71	51	134	135
Business	25	67	130	237	202	274	177	162	194	263	312	497	907	572
Educational	75	80	111	131	78	65	57	63	54	57	58	97	128	77
Government/Military	21	99	110	110	90	104	54	55	60	91	63	72	79	100
Medical/Healthcare	16	44	63	99	70	165	102	167	271	332	275	373	384	367
Total # of Breaches:	**157**	**321**	**446**	**656**	**498**	**662**	**421**	**471**	**614**	**781**	**779**	**1090**	**1632**	**1251**

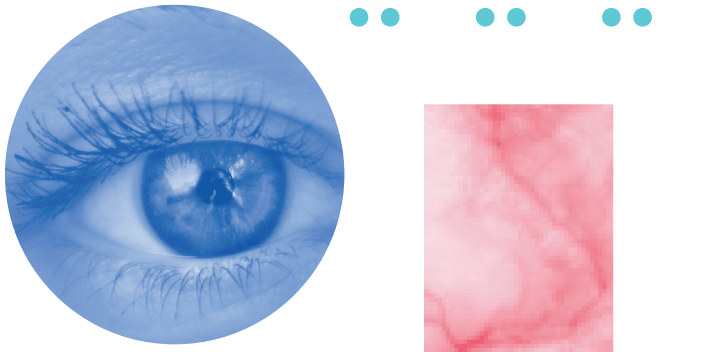
44

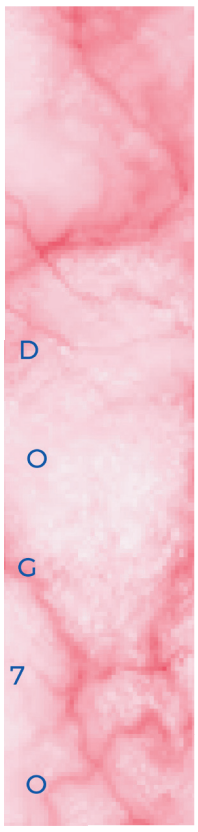
É provável que esta tendência também ocorra no Brasil, ainda mais quando se considera o quão dinâmica é a área de segurança da informação. Assim, no caso exemplificado do vazamento de prontuários médicos do hospital, a LGPD exige que os consumidores afetados sejam informados sobre o ocorrido, pois o vazamento dessa categoria de informação possui alto potencial de dano ao Titular. Ademais, quando a ANPD for definir qual sanção será aplicada, ela avaliará

44_ Identity Theft Resource Center (ITRC). ITRC Multi-Year Data Breach Chart Jan. 1, 2005-Dec. 31, 2018. 31/01/2019. Disponível em: <https://www.idtheftcenter.org/data-breaches/>. Acessado em:06/02/2019

se o Hospital adotava medidas de segurança adequadas bem como se armazenava os dados sensíveis em formato criptografado com objetivo de dificultar sua utilização em caso de vazamento. As circunstâncias do caso podem levá-la a aplicar sanções mais brandas, como no caso de o Hospital possuir um robusto programa corporativa de privacidade e proteção de dados, com políticas adequadas e implementadas, adotando as recomendações sobre segurança a serem desenvolvidas pela Autoridade, além de ter contribuído com as investigações. Desse modo, os detalhes técnicos explicando porque houve o vazamento serão de suma importância para a análise da ANPD e medição das sanções aplicáveis.

Nesse cenário, os consumidores também poderão exigir indenizações na própria Justiça, seja em processo individual ou coletivo. O Código de Defesa do Consumidor estabelece que o dano causado por falha de serviço deve ser indenizado, independente da comprovação da culpa do prestador. Assim, a adoção de medidas de segurança adequadas, apesar de não afastar eventuais indenizações por dano moral ou material por vazamento, provavelmente serão consideradas como um elemento essencial para diminuir seu valor.





A B Y D

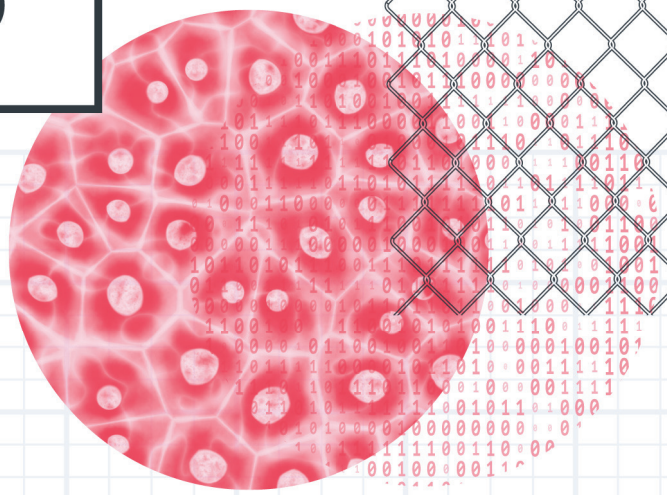
K Y W O

B S A G

2 3 4 7

H U O O

8



Melhores práticas de proteção de dados para Dados de Saúde

Uma empresa cujo modelo de negócio é a comercialização de testes genéticos está em processo de adequação à LGPD. Pensando nisso, a empresa busca orientação para implementar as melhores práticas existentes para a proteção de dados genéticos.

O caso acima envolve as melhores práticas que podem ser adotadas por uma empresa que processa dados genéticos. Conforme já foi abordado em tópicos anteriores, o tratamento de dados sensíveis envolve riscos superiores aos o do tratamento de dados pessoais normais. No caso do processamento de dados genéticos, existem riscos que são inerentes à essa atividade. Em relatório, o *Future of Privacy Forum*[45] 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;[46] **(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**[47] e outra seção sobre **governança e boas práticas**[48]. 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.

Tendo em vista que a proteção de dados pessoais é uma matéria relativamente recente em nosso ordenamento jurídico, é esperado que as autoridades competentes, como a ANPD, busquem posicionamentos de autoridades estrangeiras ao regular a matéria. Assim, hoje, a recomendação das melhores práticas para o tratamento de dados genéticos seria baseada nas regras e princípios de proteção de dados, bem como em opiniões emitidas no plano internacional sobre o tema.

É possível afirmar que as seguintes medidas provavelmente seriam classificadas como boas práticas para a empresa, considerando o tratamento de dados genéticos:

1) **Anonimização**: conforme melhor explicado em tópicos anteriores, submeter os dados a processo de **anonimização** traz uma **maior segurança** para o tratamento além de criar novas possibilidades de uso destes, uma vez que o tratamento de dados anonimizados, considerando estado da arte da tecnologia, custo e tempo, não permite a identificação, nem indireta, do titular.

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, estes precisam ser, ainda, específicos e destacados. Em se tratando de dados genéticos, caso a empresa deseje utilizar esses dados para outras finalidades (ex.: pesquisa na área

45_ FUTURE OF PRIVACY FORUM. **Privacy Best Practices for Consumer Genetic Testing Services.** Washington, Julho 2018. Página 1.

46_ Primeiro caso criminal nos EUA que utilizará family tree forensics: <https://www.wired.com/story/the-first-murder-case-to-use-family-tree-forensics-goes-to-trial/>

47_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 46 e seguintes.

48_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 50 e seguintes.

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,[49] 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**, por exemplo, um documento escrito com linguagem excessivamente técnica ou com hipóteses genéricas de tratamento dificilmente será considerado adequado. 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 base legal utilizada de acordo com a categoria do dado, a forma pela qual os Titulares poderão exercer os seus direitos, as hipóteses de compartilhamento dos dados, entre outros pontos. Todavia, um simples documento com a Política de Privacidade, para o caso de dados sensíveis, como os genéticos, provavelmente não seria considerado suficiente para legitimar um tratamento com base no consentimento. Outras formas de interação do indivíduo e de apresentação da informação seriam mais adequadas, como às que permitem ações específicas do titular dos dados para concordar com determinadas finalidades, além de informes separados.

4) **Compartilhamento**: é recomendável que a empresa, a menos que por autorização ou solicitação expressa do titular, não compartilhe os dados genéticos com terceiros, em razão da sensibilidade destes, sendo restringido tal compartilhamento para fins de obtenção de vantagem econômica, salvo para as hipóteses relacionadas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluindo serviços auxiliares de diagnose e terapia. Também é permitido o compartilhamento de dados de saúde para realizar a portabilidade dos dados quando solicitada pelo titular, e para permitir as transações financeiras e administrativas relacionadas ao serviços elencados anteriormente[50]. Entretanto, não é permitido que as operadores de planos privados de assistência à saúde realizem tratamento[51] de dados de saúde (p. ex. processamento, compartilhamento, classificação, etc) para realizar (i) a seleção de riscos na contratação de qualquer modalidade, e na (ii) a contratação e exclusão de beneficiários.[52]

5) **Segurança**: o tratamento de dados genéticos exige um alto nível de segurança e confidencialidade. Assim, é recomendável a adoção de uma política de segurança da informação adequada (controle de acesso à base de dados, criptografia, etc.) e programas corporativos de governança de proteção de

49_ UNIÃO EUROPEIA. Working Party 29. Opinion 02/2013 on apps on smart devices. Disponível em <https://www.pdpjournals.com/docs/88097.pdf>. "In some cases users are able to give a granular consent, where consent is sought for each type of data the app intends to access. Such an approach achieves two important legal requirements, firstly of adequately informing the user about important elements of the service and secondly asking for specific consent for each. The alternative approach of an app developer asking its users to accept a lengthy set of terms and conditions and/or privacy policy does not constitute specific consent."

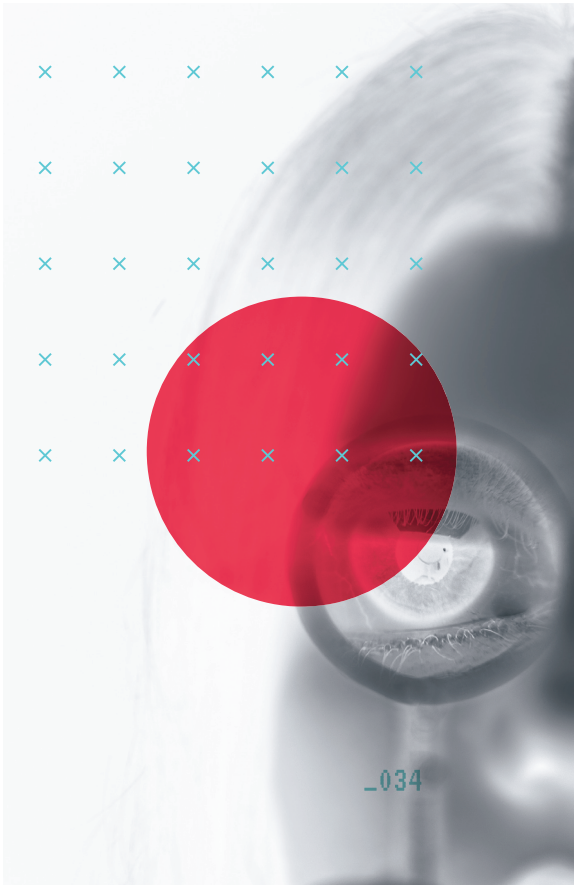
50_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º, §4º.

51_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 5º, X.

52_ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 11º, §5º.

dados robustos.

Por último, o tratamento de dados genéticos 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. A adoção de metodologias de *privacy by design*, privacidade desde a concepção, também é altamente recomendável, devendo ser uma boa prática cogente.



9

Relatórios de Impacto à Proteção de Dados em empresas de saúde

intersecção entre GDPR e LGPD

Um hospital, diante da iminente entrada em vigor da LGPD, resolveu identificar como mensurar os eventuais riscos aos titulares de dados de saúde quando estes fossem tratados por meio de soluções de Inteligência Artificial, como para fins de medicina preventiva. Para tanto, gostaria de saber como os Relatórios de Impacto à Proteção de Dados podem ajudar nessa tarefa.

Uma rede de hospitais particulares, com o intuito de se adiantar à implementação da Lei Geral de Proteção de Dados brasileira (LGPD), buscou se informar sobre quais medidas deveria adotar para estar em compliance com a nova legislação. Uma das preocupações centrais do hospital está relacionada à implementação de soluções de Inteligência Artificial (IA) para análise automática dos prontuários médicos de seus pacientes, dando uma maior eficiência para diagnósticos de certas doenças. O jurídico da rede de hospitais verificou que a nova lei menciona a elaboração de um "relatório de impacto à proteção de dados pessoais" (Relatório) para fins de mensuração de riscos existentes no tratamento de dados pessoais. Nesse contexto, a rede de hospitais busca saber se ela deve realizar tal relatório, quais seriam os elementos que ele deveria analisar, e quais seriam os benefícios que a elaboração desse relatório pode trazer à empresa.

A LGPD faz menção à elaboração de um relatório para avaliar o impacto de um determinado tratamento de dados pessoais. Tal documento tem como inspiração a legislação europeia de proteção de dados (GDPR). Na Europa, o *data protection impact assessment* (DPIA), uma espécie de metodologia específico determinada por lei do gênero *Privacy Impact Assessment* (PIA), busca analisar como se dá o tratamento dos dados pessoais em relação a um tipo específico de tratamento, para que possam ser identificados os possíveis riscos aos direitos do titulares, e, a partir disso, verificar quais mecanismos de mitigação podem ser adotados. A GDPR enfatiza que o DPIA deve ser utilizado, principalmente, no momento anterior à aplicação de um novo processo de tratamento de dados, e, especialmente, se o mesmo for utilizar novas tecnologias que tenham alta probabilidade de oferecer altos riscos aos direitos e liberdades dos titulares, como possível no caso de tratamento por meio de algoritmos de inteligência artificial.

A lei brasileira, entretanto, não define claramente quais são os casos em que seria obrigatório a produção do análogo Relatório de Impacto à Proteção de Dados Pessoais, indicando somente que a ANPD poderá requisitar que o responsável pelo tratamento, o controlador, o faça.[53] Os casos mencionados na lei sobre a requisição do relatório pela ANPD são: (i) o controlador dos dados pessoais utiliza como base legal do tratamento o legítimo interesse[54]; (ii) o tratamento envolve dados sensíveis[55]; (iii) o tratamento é feito por órgãos públicos[56]; ou para (iv) qualquer controlador que realize um tratamento de dados pessoais, inclusive de dados sensíveis[57].

A LGPD define que o relatório de impacto deve conter "a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". Nesse sentido, os elementos mínimos que um relatório deveria analisar são:

i) a descrição dos tipos de dados coletados;

ii) a metodologia utilizada para a coleta;

iii) as medidas de segurança da informação adotadas; e

iv) análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

53_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigos 5º,XVII; 10, §3º; 38; e 55-J, XIII.

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 38.

56_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 32.

57_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 38.

Apesar de a LGPD não esgotar os elementos obrigatórios que um Relatório deve conter, a semelhança da GDPR, ela estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) deve editar regulamentos e procedimentos sobre a produção desses Relatórios.[58] É possível cogitar que haja exigências diferentes a depender do setor econômico envolvido. Ademais, de forma semelhante à GDPR, como os elementos mínimos exigidos na LGPD são amplos e genéricos, é possível que um Relatório seja escalável, sendo possível que pequenas e médias empresas os desenvolvam de forma proporcional às características do tratamento por elas realizado. Esta característica acaba por equilibrar o fardo regulatório para empresas de tamanhos diferentes.

Dessa perspectiva, o Relatório serve tanto (i) para auxiliar os agentes a adotar as medidas adequadas para estarem em conformidade com a lei, quanto (ii) para efetivamente demonstrar que tais agentes estão em conformidade. Assim, o relatório de impacto à proteção de dados serviria para equilibrar tanto os interesses econômicos das empresas, quanto para a proteção dos direitos do titular.

Binns, que é um pesquisador do tema, afirma que o DPIA não se enquadra como uma ferramenta de autorregulação de uma empresa (*self-regulation*), mas como um instrumento de meta-regulação (*meta regulation*).[59] 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 elemento que facilita o *compliance* com as leis de proteção de dados pessoais é o entendimento de que é possível realizar apenas um Relatório para mais de uma operação de tratamento desde que elas sejam semelhantes, e ofereçam riscos similares aos titulares dos dados.

Independente da requisição direta da ANPD, o Relatório é uma ferramenta fundamental para que uma empresa possa implementar um processo de conformidade com a LGPD, seja em relação aos tratamentos já realizados, ou para desenvolver um novo serviço ou produto. A elaboração de um Relatório na fase de desenvolvimento também auxilia com que o conceito de *privacy by design* seja implementado na prática.

Outro ponto interessante de se destacar baseado na experiência europeia, e que provavelmente também será adotado no Brasil, é que não existe uma única metodologia de produção de um relatório de impacto à proteção de dados pessoais. Apesar de os objetivos das diversas metodologias serem os mesmos, existem vários *frameworks* diferentes elaborados pelas Autoridades de Proteção de Dados de cada país europeu, por organizações privadas como a ISO, e modelos desenvolvidos especificamente para analisar determinados produtos e serviços (p. ex. uso de RFID, *smart grids*, medicina diagnóstica, entre outros).

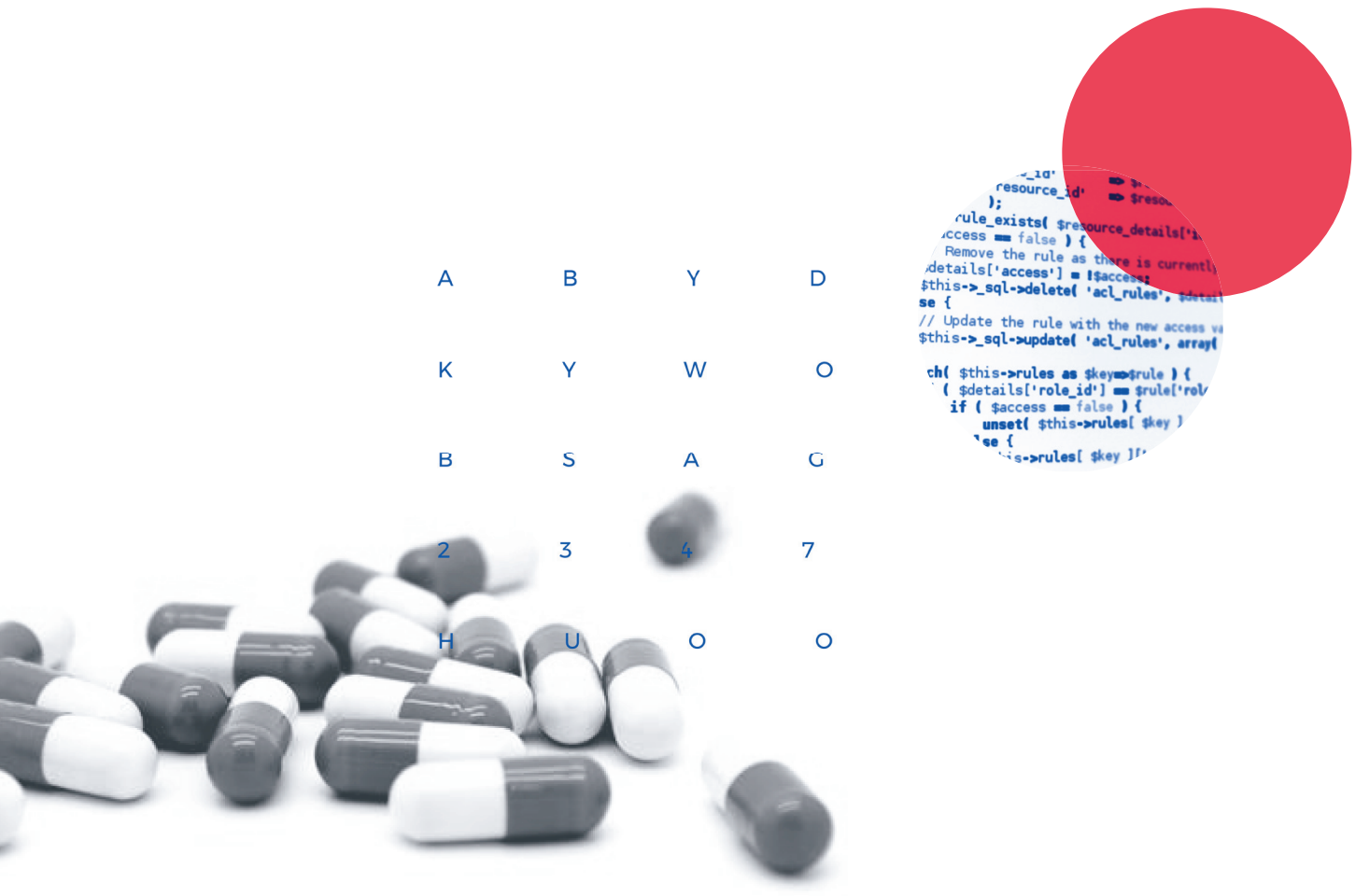
Por fim, é necessário que um Relatório seja revisado periodicamente, principalmente quando houver alterações significativas na forma do tratamento ou modelo de negócio que

58_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 55-J, XIII.

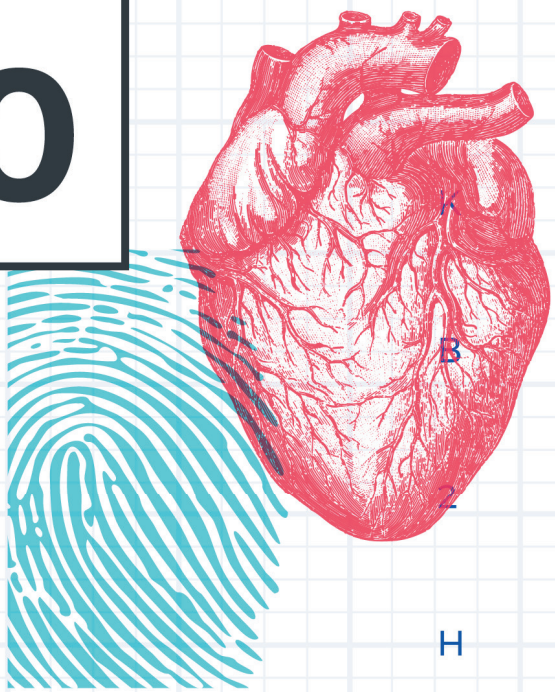
59_BINNS, Reuben. Data Protection Impact Assessments: A Meta-Regulatory Approach. Business Horizons. *International Data Privacy Law, Vol. 7(1). 2017.*

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 Relatório 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.



10



Algoritmos de Inteligência Artificial e a Proteção de Dados Pessoais

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 o os diversos tipos de algoritmos de inteligência artificial existentes atualmente referem-se ao conceito de IA[60] no sentido estrito (*narrow AI*), o qual pode ser definido como sistemas que possuem 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.[61] 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.

Atualmente, não existem regulações claras no Brasil sobre o uso de algoritmos de Inteligência Artificial para diagnósticos na saúde. A Agência Nacional de Vigilância Sanitária (ANVISA) apenas possui algumas normas esparsas sobre softwares de saúde e os procedimentos administrativos necessários para que tais produtos possam ser utilizados no país. A Agência classifica os produtos médicos conforme o risco que apresentam à saúde, exigindo que seja feita um cadastro ou registro conforme a classificação.[62] De forma simplificada, o **registro** é um procedimento no qual a Agência reconhece que determinado produto está adequado à legislação sanitária, sendo um controle prévio à comercialização, e que deve ser concedido em 90 dias. Já o **cadastro** refere-se a produtos isentos de registro, sendo um procedimento mais simples que o primeiro.

Apesar da ausência de regulação clara, a ANVISA elaborou um guia orientativo para softwares de saúde na **Nota Técnica nº 4 de 2012**. Esta nota apresenta três categorias de software de saúde, sendo possível classificar um algoritmo de IA para diagnóstico na categoria de "software produto para a saúde (medical device), por si mesmo". Esta categoria abrange produtos que não precisam de um '*hardware*' classificado como "produto para a saúde" para serem utilizados, sendo, por padrão, executados em um computador isolado. No caso de o software estar "embarcado" em um equipamento específico, como uma máquina de tomografia, por exemplo, o software deve ser registrado/cadastrado de acordo com a própria classificação do equipamento médico. O uso irregular de softwares de saúde que exigem registro ou cadastro é passível de sanções administrativas, como advertência, multa, cancelamento de autorização para funcionamento da empresa, entre outros.[63] Também é importante destacar que a **Agenda Regulatória 2017-2020 (AR)** da ANVISA estabeleceu como uma de suas metas prioritárias a "regularização de software como dispositivo médico". Esse procedimento é importante pois a AR é a primeira etapa do processo regulatório da Agência.

Uma possível dificuldade regulatória no âmbito da aprovação do uso de IAs pela ANVISA decorre do fato de esses algoritmos possuírem a capacidade de se desenvolverem conforme vão sendo treinados com novos dados.[64] Desse modo, uma IA é diferente de um software padrão, pois, no segundo, os critérios de tomada de decisão são previamente inseridos pelos programadores, só sendo modificados caso um ser humano altere

60_Neste texto especificamente os termos inteligência artificial, algoritmo e software são usados de forma intercambiável.

61_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.

62_BRASIL. Agência Nacional de Vigilância Sanitária (ANVISA). Resolução da Diretoria Colegiada (RDC) nº 185/2001

63_BRASIL. Lei nº 6.437, de 20 de agosto de 1997. Artigo 2º.

64_TEICH, David A. Artificial Intelligence (AI), Healthcare and Regulatory Compliance. Forbes. 20 de maio de 2018. Disponível em: <https://bit.ly/2TFUdQK>. Acessado em: 07/02/2019.

diretamente sua programação. Assim, é possível que as agências reguladoras envolvidas tenham que adotar metodologias de acompanhamento periódico dos algoritmos autorizados, ou exigir que os agentes comprovem a realização de testes frequentes que garantam o acompanhamento da qualidade dos softwares.

A Lei Geral de Proteção de Dados Pessoais apresenta diversos dispositivos que serão aplicáveis ao uso de algoritmos de IA para diagnósticos. Um possível ponto de atenção será em como efetivar o princípio da transparência aos titulares dos dados em relação ao uso de IA para tomada de decisões. 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"[65], o qual foi inspirado em uma norma semelhante do Regulamento Geral de Proteção de Dados Europeu. Este direito deverá ter relevância, pois poderá ser uma das formas de fiscalizar se determinadas decisões automatizadas estão sendo afetadas por vieses discriminatórios ilícitos ou abusivos. 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 algoritmos de IA frequentemente apresentam um problema de caixa preta (*black box problem*). Este termo refere-se a uma característica técnica relativa à incapacidade dos programadores em explicarem como uma IA chegou a determinado resultado.[66] Este problema afeta diretamente os limites de um possível direito a explicação e como ele será efetivado na prática.

Os titulares afetados por IAs também possuem o direito de requisitar uma revisão das decisões baseadas unicamente no tratamento automatizado de seus dados, que pode ser realizado por uma pessoa natural, conforme regulamentação da ANPD que deve considerar o porte da entidade e o volume de operações de tratamento[67]. 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[68], como no exemplo do médico.

Outro ponto a ser destacado é a necessidade dos desenvolvedores de IA de obterem uma das bases legais da LGPD para utilização de dados pessoais que venham a ser utilizados para o treinamento de algoritmos. Assim, por exemplo, se um Plano de Saúde desenvolver um projeto para criar um IA de diagnóstico de câncer através do uso de tomografias de seus pacientes, provavelmente seria necessário obter o consentimento dos mesmos para tal utilização, considerando que esta é a hipótese mais segura juridicamente para tratamento de dados sensíveis. Caso o uso de algoritmos de IA possam ser necessários para adequada tutela da saúde, talvez seja possível se valer dessa base legal, mas como exceção ao consentimento, não como regra ou opção. Outra possiblidade seria que esses dados fossem anonimizados de forma

65_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 20º.

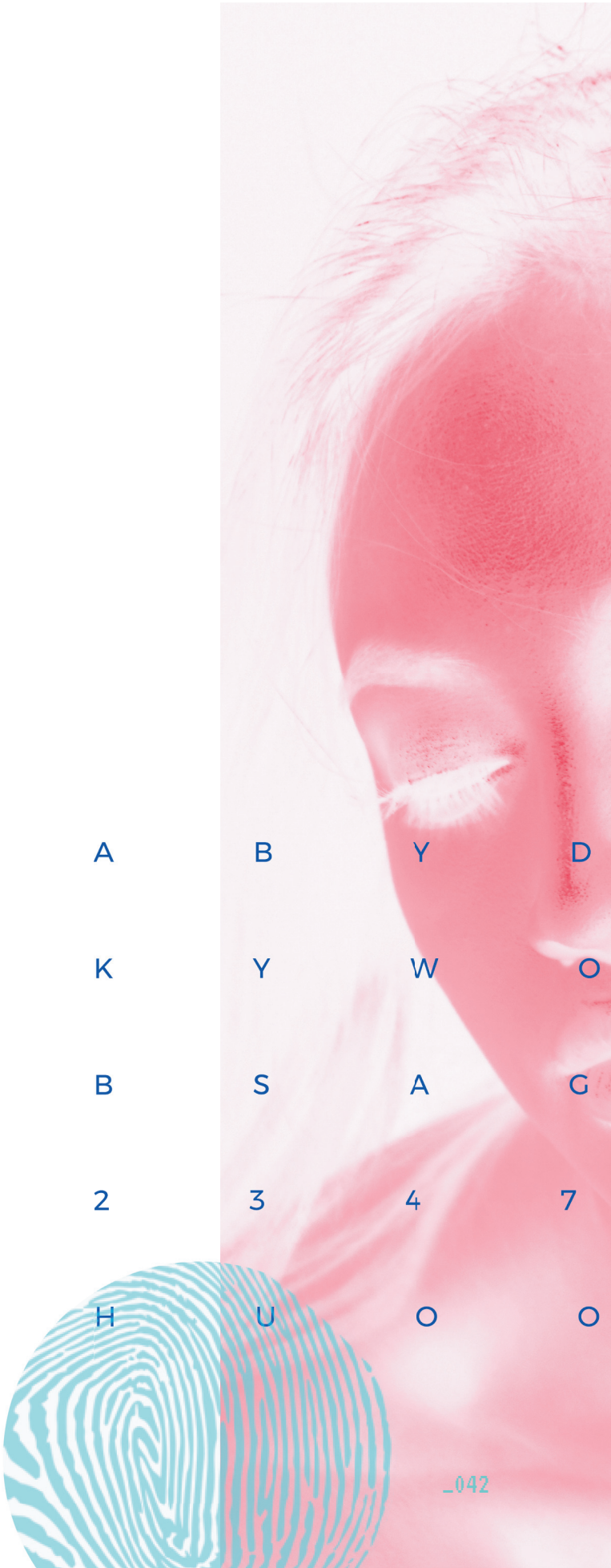
66_KNIGHT, Will. The Dark Secret at the Heart of AI: No one really knows how the most advanced algorithms do what they do. That could be a problem. MIT Technology Review. Edição de Maio/Junho 2017. Disponível em: <https://bit.ly/2otrSjZ>. Acessado em: 07/02/2019.

67_BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Artigo 20º, § 3º.

68_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.

a deixarem de ser considerados dados pessoais pela LGPD, o que permitiria uma maior liberdade na sua utilização.

Em relação ao caso hipotético, a startup deve buscar registrar ou cadastrar seu algoritmo na ANVISA, em conformidade com as exigências estabelecidas pela Agência. A empresa também deve verificar se ela possui as devidas bases legais para uso dos dados utilizados no treinamento de sua IA, no caso de os mesmos se enquadrarem no conceito de dado sensível da LGPD. Caso ela deseje obter os dados de treinamento de terceiros, estes devem ser anonimidades, devido às limitações ao compartilhamento de dados sensíveis para fins econômicos da LGPD. É possível, entretanto, que a ANPD entenda no futuro que o compartilhamento de dados sensíveis para treinamento de algoritmos possa ocorrer num contexto de adequada prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, caso a IA venha a ser utilizada nesse contexto. A startup também deve se atentar a como efetivar o princípio da transparência aos usuários, de forma fornecer informações mínimas sobre a lógica decisória, e ao mesmo tempo proteger sua propriedade intelectual.



Conclusão

A área da saúde será uma das mais atingidas pela 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, o setor passará por profundas alterações. É necessário que os entes regulados se preparem e se antecipem à entrada em vigor da lei, que acontecerá em agosto de 2020, 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.

Glossário

ANONIMIZAÇÃO

Processo pelo qual os dados não permitem mais identificar o titular a quem originalmente se referiam, utilizando meios técnicos razoáveis e disponíveis na época de seu tratamento.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados.

BASE LEGAL

É a hipótese que permite o tratamento de dados pessoais, considerando a categoria do dado e a finalidade do tratamento.

DADO DE SAÚDE

É qualquer informação referentes à saúde, à vida sexual, ao dado genético ou biométrico. Esse conceito engloba, também, dados pessoais que, num primeiro momento, podem não parecer ser de saúde, mas que, dentro de um contexto, podem permitir inferir dados de saúde.

DADO PESSOAL

É qualquer informação relacionada a pessoa natural identificada ou identificável.

DADO SENSÍVEL	São os dados pessoais relacionados 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 à uma pessoa.
GDPR	Regulação europeia de proteção de dados pessoais.
LGPD	Lei Geral de Proteção de Dados, Lei nº 13.709/18.
PSEUDONIMIZAÇÃO	Processo por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional desassociada.
TERMO DE CONSENTIMENTO	Instrumento por meio do qual o controlador dos dados obtém o consentimento do titular do dado para finalidades específicas de tratamento.
TITULAR DOS DADOS	Pessoa a quem os dados pessoais se referem.

Sobre Baptista Luz Advogados

Com mais de uma década de atuação, nossa especialidade é apresentar soluções efetivas e ideias inovadoras para as questões jurídicas de nossos clientes, parceiros e empreendedores.

Com profissionalismo e experiência, nosso escritório oferece assessoria legal de alta qualidade por meio de atendimento personalizado, em que o cliente recebe todo o suporte necessário com precisão e clareza.

Siga-nos nas redes sociais

BRASIL

São Paulo
Rua Ramos Batista, 444 / 2° Andar
Vila Olímpia / São Paulo / SP / Brasil
tel +55 11 3049 7950

Florianópolis
Rodovia SC 401, Km 4 / Saco Grande /
Florianópolis / SC
tel +55 48 3036 0294

Londrina
Rua Ayrton Senna da Silva, 300 /
Sala 1801, Torre 1 / Gleba Palhano
Londrina / PR
tel +55 43 3367 7050

USA

Miami
78 SW 7th Street Suite 500
Miami / FL 33130 / US
tel +1 (786) 622 2002

Acesse nosso site:
baptistaluz.com.br