NÚMERO 1 / 10

A Year in Privacy

BAPTISTALUZ

Autores

Adriane Loureiro Novaes

Lucas Oliveira Balsamão Magela

Luiz Felipe Sundfeld Ibrahim

Matheus Botsman Kasputis

Odélio Porto Júnior

Coordenador e Revisor

Fernando Bousso

Projeto Gráfico

Fernanda Muchon

Laura Klink

Lucas Bittencourt

índice

01 A interpretação da base da tutela da saúde e os desafios para inovação na área da saúde

Voltar para o índice

A interpretação da base da tutela da saúde e os desafios para inovação na área da saúde

Autora

Adriane Loureiro Novaes

1_Introdução

No Brasil as empresas pertencentes ao ecossistema da saúde vêm passando por uma profunda transformação digital e os dados são facilitadores fundamentais para essa transformação e inovação. Impulsionado pelos avanços da computação, inteligência artificial e uma base de dados em rápida expansão, o ecossistema da saúde no Brasil passa por uma transformação digital com enorme potencial para aprimorar muitos aspectos da saúde, em benefício do paciente e da população brasileira em geral.

A medicina personalizada, por exemplo, é uma abordagem emergente que usa dados gerados por novas tecnologias para entender melhor as características de um indivíduo e fornecer tratamentos individualizados. Novas tecnologias permitem o uso dos dados de saúde (como perfil molecular, diagnóstico por imagem, dados de ambiente e estilo de vida) para ajudar médicos e cientistas a entender melhor as doenças e encontrar meios para preveni-las, diagnosticá-las e tratá-las.

Mas existem algumas barreiras que separam os dias atuais do futuro no qual os dados de saúde e as novas tecnologias são efetivamente aproveitadas para proporcionar melhorias em muitos aspectos da nossa saúde.

Dentre tais barreiras podemos destacar os desafios técnicos e organizacionais para compartilhamento e uso dos dados nas instituições de saúde. Além de ser um setor altamente regulado, com imposições normativas a todas as partes que compõem o ecossistema, o setor da saúde ainda tem que lidar com

questões técnicas relacionadas aos sistemas obsoletos e que não conversam entre si, especialmente por armazenar dados em formatos que não são facilmente utilizados por outros sistemas. Como se não bastasse, por uma característica específica dos seus serviços, os dados de saúde estão armazenados em diversos lugares, espalhados por diversos agentes que compõem o ecossistema da saúde.

Progressos significativos estão sendo feitos para que uma nova norma global denominada Fast Healthcare Interoperability Resources (FHIR) ganhe força. Este importante padrão descreve formatos de dados e uma Application Programming Interface (API) para o compartilhamento de registros eletrônicos de saúde, criado pela organização de padrões de saúde Health Level Seven International (HL7)[1] .

Outra tecnologia que tem grande potencial para que o compartilhamento de dados de saúde seja realizado pelos agentes do ecossistema para melhorar a qualidade do atendimento, reduzir custos e melhorar a experiência dos pacientes e profissionais da saúde, é o Blockchain[2] [3].

Outra barreira que separa os dias atuais de um futuro com avanços tecnológicos é a falta de regras claras sobre o uso permitido dos dados de saúde e as implicações éticas e sociais para o uso de novas tecnologias. A Lei 13.709/2018 (a Lei Geral de Proteção de Dados Pessoais ou LGPD) traz diversas obrigações que visam proteger dados pessoais de saúde, bem como os direitos e liberdades dos titulares de tais dados. Contudo, especialmente no que diz respeito ao tratamento de dados pessoais de saúde, alguns conceitos devem ser interpretados com cautela pela Autoridade Nacional de Proteção de Dados ("ANPD"), de forma a não impedir o avanço tecnológico e científico do setor da saúde.

A base legal da tutela da saúde trazida pela LGPD, conforme redação alterada pela Lei nº 13.853/2019[4] , oferece uma oportunidade para o uso dos dados de saúde para viabilizar a realização de pesquisas clínicas e desenvolvimento tecno-

[1]HEALTH LEVEL SEVEN INTERNATIONAL. Especificação FHIR (Fast Healthcare Interoperability Resources). Disponível em <https://www.hl7.org/fhir/overview.html>. Acesso em: 19.01.2022.

[2]De acordo com a European Commission, "New decentralised digital technologies such as blockchain offer a further possibility for both individuals and companies to manage data flows and usage, based on individual free choice and self-determination. Such technologies will make dynamic data portability in real time possible for individuals and companies, along with various compensation models". EUROPEAN COMMISSION. A European Strategy for data. COMM (2020) 66 final, p. 11. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>. Acesso em: 19.01.2022.

[3]De acordo com Tatiana Revoredo e Rodrigo Borges, "Um dos aspectos mais empolgantes da arquitetura Blockchain é que ela foi projetada para ser inteiramente descentralizada, distribuída" e apontam "a arquitetura Blockchain como a mais segura para proteção dos dados". BORGES, Rodrigo; REVOREDO, Tatiana. Criptomoedas no cenário internacional. São Paulo, SP. 2018.

lógico nesta área, trazendo, como consequência, benefícios sociais significativos.

Contudo, para se valer dessa base legal, é importante ter discussões de como e em quais circunstâncias esses dados de saúde podem ser utilizados, delineando os usos proibidos e identificando métodos que dão aos pacientes o devido controle sobre seus dados. E é sob essa perspectiva que nos debruçaremos adiante neste artigo.

2_Os limites impostos pela LGPD

Em discussões com pacientes, pesquisadores, inovadores tecnológicos e reguladores do segmento da saúde, o tema de privacidade e proteção de dados sempre são constantes. O motivo é que existem claros desafios no equilíbrio entre a necessidade em resguardar a privacidade e a proteção dos dados pessoais do indivíduo vis-à-vis a promoção de pesquisas e inovação no segmento da saúde.

Qualquer discussão sobre privacidade e proteção de dados no Brasil deve começar pela LGPD. A LGPD traz diversas regras e obrigações relacionadas à privacidade e proteção de dados pessoais[5], tanto em meios online quanto offline, sendo aplicável a praticamente qualquer organização, seja ela pública ou privada, com ou sem fins lucrativos, independentemente do setor econômico a que pertença.

A LGPD proporciona relevante expectativa de segurança jurídica às organizações e à população no que diz respeito ao tratamento[6] de dados pessoais, além de definir as bases legais[7] que autorizam tais tratamentos e aumentar o rol de direitos dos titulares de dados, prevendo, por exemplo, o direito de acesso facilitado às informações referentes à forma de uso dos dados, o direito de exclusão dos dados em determinadas situações, o direito à porta-

[4]BRASIL. Lei nº 13.853/2019. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2>. Acesso em: 19.01.2022.

[5]Dado pessoal é qualquer informação relacionada a uma pessoa natural identificada ou que possa vir a ser identificada (art. 5º, I, da LGPD); essa definição deve ser entendida de modo a incluir, ainda, números identificativos, dados de localização, identificadores eletrônicos, dados sensíveis (definidos no art. 5º II da LGPD), ou qualquer dado que, quando combinado com outras informações, seja capaz de identificar uma pessoa natural, torná-la identificável ou, ainda, individualizá-la.

[6]Tratamento é toda operação realizada com dados pessoais, como as que se referem a atividades de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X, da LGPD).

[7]Bases legais são hipóteses trazidas pela LGPD que autorizam o tratamento dos dados pessoais (arts. 7º e 11, da LGPD).

bilidade dos dados, o direito à revisão de decisões automatizadas, o direito à revogação do consentimento, entre outros.

A LGPD também cria a categoria de dados pessoais sensíveis[8], que é uma categoria de dados para os quais, em razão de seu maior potencial discriminatório e criticidade, são estabelecidos requisitos mais elevados para o seu tratamento. Dentre tais dados sensíveis estão os dados de saúde.

Contudo, a LGPD ainda precisa ser regulamentada em diversos aspectos, pela ANPD, especialmente no que se refere ao tratamento de dados pessoais sensíveis para fins de pesquisa, desenvolvimento de novos produtos e inovação na área da saúde.

2.1_Análise das bases legais aplicáveis à realização de pesquisas, desenvolvimento de novos produtos e inovação na saúde

Para permitir o avanço tecnológico e científico do setor da saúde é muito comum que as empresas se utilizem de dados pessoais sensíveis coletados por meio da prestação de serviços de saúde, seja online ou presencial, para realizar pesquisas ou o desenvolvimento de novos produtos – o que é denominado de uso secundário dos dados, já que o uso do dado vai além daquele relacionado à prestação dos serviços de atenção primária. Contudo, em respeito aos princípios da finalidade e da adequação trazidos pela LGPD, todo e qualquer tratamento de dados pessoais deve ser compatível com as finalidades para as quais os dados pessoais foram originalmente coletados, sendo vedada a possibilidade de tratamento posterior de forma incompatível com o que foi informado ao titular e em desacordo com o contexto do tratamento.

Desta forma, para viabilizar a realização de pesquisa, desenvolvimento de novos produtos e inovação na área da saúde, o ideal é a adoção de técnicas de anonimização dos dados pessoais sensíveis, que, apesar de não permitir a identificação dos titulares, podem ser úteis e ter um alto valor para o mercado, além de afastar a aplicação das obrigações trazidas pela LGPD.

Contudo, a anonimização nem sempre permitirá que as finalidades pretendidas sejam alcançadas. Para o avanço da medicina personalizada, por exem-

[8]Dados sensíveis são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5, II, da LGPD).

plo, é necessário combinar a maior quantidade de dados de saúde possível para que os médicos e pesquisadores possam obter uma melhor imagem da doença e determinar o tratamento mais apropriado para o paciente. Nessas situações, em que não há a possibilidade de anonimização dos dados, devem ser observadas todas as regras da LGPD.

Apesar da LGPD não estabelecer hierarquia entre as bases legais, é certo que, no que se refere ao tratamento de dados sensíveis, existe notável preferência pelo uso da base legal do consentimento, sendo as demais bases legais aplicáveis somente nas hipóteses de impossibilidade prática de obtenção de consentimento dos titulares, e apenas quando o tratamento se mostrar indispensável para o cumprimento das finalidades descritas no inciso II do artigo 11 da LGPD. Isso significa dizer que, quando as empresas pretenderem tratar dados sensíveis no contexto de suas atividades, o consentimento dos titulares deve ser buscado sempre que possível.

Contudo, exigir o consentimento para tratamento dos dados para fins de pesquisa, desenvolvimento de novos produtos e inovação na área da saúde pode ser inviável pois (i) o consentimento obtido nesses casos é genérico e sem finalidades determinadas, já que não se sabe o produto e/ou inovação que será desenvolvido com os dados pessoais; e (ii) o consentimento pode não ser considerado devidamente informado, conforme exigido pela LGPD, uma vez que novos produtos e tecnologias são complexas e difíceis de serem explicadas ao cidadão médio; permitindo que, em qualquer caso, o consentimento seja considerado nulo[9].

Quando o tratamento envolve apenas dados pessoais comuns, as empresas têm a oportunidade de se respaldar na base legal do legítimo interesse para tais finalidades. Contudo, essa não é uma possibilidade quando o tratamento envolve dados sensíveis.

Para realizar a devida avaliação da impossibilidade de aplicação do consentimento em cada caso concreto, é sugerida a realização de um **Teste de Aplicação do Consentimento para Dados Sensíveis** (modelo estruturado e desenvolvido pelo Baptista Luz Advogados, disponibilizado aqui) no qual se verifica se o consentimento, no caso concreto, é possível de ser obtido considerando todos os critérios exigidos pela LGPD.

[9]Art. 8º, §4º, da LGPD: O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

Uma vez identificada a inviabilidade de obtenção do consentimento para as finalidades secundárias discutidas neste ensaio, deve-se avaliar a possibilidade de aproveitamento das demais bases legais trazidas pela LGPD[10].

Contudo, de pronto, é possível afirmar que nenhuma de tais bases legais parece ser diretamente adequada aos propósitos ora discutidos, ou seja, de realização de pesquisas e de desenvolvimento de novos produtos, o que pode ser uma grande barreira para o avanço tecnológico e científico do setor da saúde.

A base de realização de estudos por órgãos de pesquisa, por exemplo, tem suas limitações. De acordo com a LGPD, órgão de pesquisa é qualquer órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras. Esta base legal, portanto, não pode respaldar o tratamento de dados pessoais de empresas privadas com fins lucrativos, que também exercem um papel ativo e relevante no Brasil na realização de pesquisas e desenvolvimento de novos produtos.

O mesmo ocorre com a base legal de proteção da vida, que deve respaldar o tratamento de dados pessoais efetivamente necessários à proteção da vida do titular ou de terceiros, sendo que a interpretação mais razoável da aplicação dessa base legal ocorre quando o titular ou terceiro se encontra em iminente perigo de vida (por exemplo, situações em que o paciente chega ao hospital em estado de emergência; ou em casos de pandemia, como ocorre com a COVID-19), o que não parece ser o caso, portanto, das finalidades que buscam um avanço tecnológico e científico.

Portanto, dentre as bases legais listadas, a única que deixa margem para interpretações para o tratamento secundário dos dados pessoais de saúde é, justamente, a base legal de tutela da saúde que, portanto, deve ser interpretada com cautela pela ANPD, de forma a não impedir a inovação no setor da saúde, como será abordado a seguir.

[10]De acordo com o artigo 11, inciso II, da LGPD, o tratamento de dados sensíveis poderá ocorrer sem o consentimento do titular nas hipóteses em que for indispensável para "a) cumprimento de obrigação legal ou regulatória pelo controlador; b) execução de políticas públicas previstas em leis ou regulamentos – que só pode ser usada pela administração pública; c) realização de estudos por órgão de pesquisa; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos".

2.2_Aplicação e interpretação da base da tutela da saúde

Para a correta interpretação da base legal da tutela da saúde, vale examinar o histórico de mudanças legislativas. Em 29 de maio de 2019, foi aprovada a Medida Provisória nº 869/2018, que trouxe diversas alterações à LGPD, dentre elas a redação do artigo 11, inciso II, alínea f. Antes da alteração, referida alínea permitia tratamento de dados pessoais sensíveis sem o consentimento quando fosse indispensável para a "tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias".

Com a alteração – conforme atual redação da LGPD[11]- houve um alargamento do escopo para permitir que referida base legal seja utilizada não somente no contexto de procedimentos realizados por profissionais da saúde e entidades sanitárias, mas também para permitir a prestação de **serviços de saúde no geral.**

Aliado a isso, diferentemente da base legal da proteção da vida que menciona expressamente que a proteção deve ser da vida do titular ou de terceiros, a redação da base legal da tutela da saúde deixa o escopo de aplicação amplo, o que permite a interpretação de que referida base legal visa tutelar a saúde não só do titular dos dados, mas da sociedade de maneira geral.

Com essa interpretação, seguindo a mesma lógica do GDPR[12] – lei que inspirou a redação atual da LGPD – e das regulamentações específicas sobre o assunto que têm sido adotadas pelos Estados-Membros[13], as empresas poderiam utilizar dados pessoais de saúde para fins de pesquisa, elaboração de estatísticas e desenvolvimento de novos produtos com base na tutela da saúde do titular e da sociedade como um todo.

Em paralelo, a ANPD poderá traçar diretrizes ou desenvolver um código de conduta para estabelecer como e em quais circunstâncias esses dados de saúde podem ser utilizados, delineando os usos proibidos e identificando métodos que dão aos titulares o devido controle sobre os seus dados, além de garantir que seus direitos e liberdades sejam respeitados.

Por meio de uma abordagem colaborativa, com o apoio dos diferentes stake-

[11]Art. 11, inciso II, alínea f, da LGPD: tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

[12]Em recente parecer publicado pela European Data Protection Supervisor, a Preliminary Opinion 8/2020, a EDPS se manifestou no sentido de não considerar o consentimento como a base legal mais adequada para o uso secundário dos dados pessoais de saúde, e sim a base legal relacionada ao interesse público (art. 6 (1)(e) e art. 9 (2)(i) da GDPR) e a base legal relacionada à realização de pesquisas (art. 9 (2)(j) da GDPR). Disponível em <https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en>. Acesso em 19.01.2022.

holders do setor, é possível criar uma diretriz ou um código de conduta sobre o tratamento de dados pessoais de saúde que inclua:

• A tutela da saúde como base legal para o tratamento secundário de dados pessoais de saúde, além de estabelecer interpretação comum das atividades que podem ser consideradas para a efetiva tutela da saúde dos titulares e da sociedade como um todo, para fins de interesse público.

• Os métodos de anonimização comuns e aceitáveis para cada circunstância específica, bem como diretrizes para o compartilhamento de dados pessoais de saúde entre controladores e técnicas de pseudonimização.

• Uma estrutura ética e de segurança robusta para a proteção dos dados pessoais de saúde, o que estimularia a confiança do paciente e garantiria que os dados identificáveis necessários para o avanço científico e tecnológico fossem tratados de forma adequada.

A elaboração de diretrizes e/ou código de conduta, que seja amplamente fiscalizado, pode proporcionar um equilíbrio das oportunidades tecnológicas emergentes com as normas de sigilo e proteção de dados já existentes. Referidas diretrizes podem proporcionar uma base de confiança adequada aos titulares, deixando mais claro os benefícios significativos que o uso amplo dos dados pessoais de saúde pode proporcionar.

3_Conclusão

Para permitir o avanço tecnológico e científico do setor da saúde é muito comum que as empresas se utilizem de dados pessoais sensíveis, coletados por meio da prestação de serviços de saúde, para realizar pesquisas ou o desenvolvimento de novos produtos e inovação – o uso secundário dos dados.

Para viabilizar o uso secundário dos dados pessoais, o ideal é a adoção de técnicas de anonimização dos dados pessoais sensíveis. Contudo, a anonimi-

[13]A Finlândia, por exemplo, estabeleceu uma lei separada sobre o uso secundário de dados pessoais de saúde, o Act on the Secondary Use of Health and Social Data, para facilitar o processamento e o acesso aos dados pessoais de saúde para orientação, supervisão, pesquisa, estatísticas e desenvolvimento no setor da saúde, além de garantir as expectativas legítimas de um indivíduo, bem como seus direitos e liberdades no processamento de tais dados. De acordo com referida legislação os usos secundários incluem: (i) a realização de pesquisa científica; (ii) a elaboração de estatísticas sobre os serviços de saúde; (iii) as atividades de desenvolvimento e inovação; (iv) a direção e supervisão pelas autoridades; (v) o planejamento e reporte pelas autoridades; (vi) o ensino; entre outros. Disponível em <https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf>. Acesso em 19.01.2022.

zação nem sempre permitirá que as finalidades pretendidas sejam alcançadas, podendo ser um empecilho para permitir o avanço tecnológico e científico do setor da saúde.

Embora a LGPD mantenha o consentimento como um controle fundamental para os titulares dos dados pessoais sensíveis, o legislador tentou flexibilizar o uso desses dados sem o consentimento do titular quando trouxe a possibilidade de aplicação de outras bases legais. O escopo ampliado da base legal de tutela da saúde, cobrindo também a prestação de serviços de saúde no geral, permite interpretar que referida hipótese legal de tratamento visa proteger não apenas o titular dos dados, mas a sociedade em geral. Isso inclui, portanto, o aproveitamento dos dados de saúde obtidos por meio da prestação de tais serviços para garantir uma adequada – e necessária – evolução no setor da saúde.

Não obstante, para controlar o uso indiscriminado dos dados de saúde, faz-se necessário o desenvolvimento de um código de conduta para estabelecer como e em quais circunstâncias esses dados podem ser utilizados, delineando os usos proibidos e identificando métodos que oferecem aos titulares o devido controle sobre os seus dados, além de garantir seus direitos e liberdades no processamento de tais dados, proporcionando um equilíbrio das oportunidades tecnológicas emergentes com as normas de sigilo e proteção de dados já existentes. Trata-se de janela de oportunidade para aproveitar os avanços significativos das novas tecnologias e uso massivo de dados pessoais de saúde, sem ferir os direitos e liberdades individuais do titular dos dados pessoais.

02 Reutilização de dados pessoais para fins de inovação

Reutilização de dados pessoais para fins de inovação

Autor

Odélio Porto Júnior

1_Introdução

Com o avanço da digitalização das economias, tem sido cada vez mais fácil e barato para as empresas acumular quantidades significativas de dados pessoais, principalmente de dados obtidos nas relações com consumidores. É comum que as empresas acabem por manter esses dados armazenados mesmo após já ter sido cumprida a finalidade de uso que justificou a sua coleta inicial (p. ex. prestar um serviço ao consumidor, efetivar uma venda etc.).

Pode-se considerar que a motivação da manutenção desses dados é, com frequência, a possibilidade de eles serem utilizados posteriormente, como, por exemplo, para a elaboração de inteligência de mercado ou desenvolvimento de novos produtos e serviços. Contudo, a Lei Geral de Proteção de Dados Pessoais brasileira ("LGPD") – Lei nº 13.709/2018 – estabelece que dados pessoais só podem ser tratados se houver uma finalidade de tratamento específica (art. 6, I e II, da LGPD).

A dificuldade se encontra no fato de que, muitas vezes, o agente de tratamento responsável gostaria de utilizar os dados para outras finalidades que podem destoar da finalidade inicial da coleta das informações. Essas finalidades posteriores estão, frequentemente, relacionadas à inovação e ao desenvolvimento de novos produtos e serviços. Assim, o objetivo desse texto é verificar se o **tratamento posterior ao cumprimento da finalidade inicial** pode ser justificado pela LGPD para fins de inovação.

2_Uso Posterior de Dados e a LGPD

O "princípio da finalidade" da LGPD estabelece que o uso de dados pessoais dever estar sempre relacionado a **propósitos específicos** e **informados ao titular**, não sendo permitido o tratamento posterior de forma **"incompatível"** com as finalidades iniciais (art. 6º, I). Nessa linha, a LGPD define que deve haver o "término do tratamento" após a finalidade de uso ter sido alcançada, por meio da eliminação ou anonimização dos dados (art. 15 e 16 da LGPD).

Apesar de o art. 16 da LGPD estabelecer algumas exceções que autorizam a utilização posterior dos dados, a lei não fornece parâmetros claros para análise do que seria a verificação de "compatibilidade" entre uma f**inalidade inicial** e uma **finalidade posterior.** No item abaixo, iremos analisar como um teste de compatibilidade entre a finalidade inicial e a posterior pode ser realizado para se verificar a adequação do uso posterior dos dados para fins de inovação.

2.1_Teste de compatibilidade

De forma semelhante à LGPD, a legislação da União Europeia (UE) de proteção de dados (General Data Protection Regulation – "GDPR" **[1]**) também limita o uso posterior de dados pessoais à compatibilidade com as finalidades iniciais (art. 5, 1[b] da GDPR). Contudo, a legislação europeia fornece critérios para verificação da compatibilidade entre a finalidade inicial e a posterior de tratamento, sendo eles (art. 6, 4, da GDPR):

- se existe alguma conexão entre a nova finalidade e a finalidade inicial de uso dos dados;

- o contexto da coleta dos dados, principalmente quanto ao tipo de relação que o agente de tratamento possui com o titular;

- os tipos de dados pessoais utilizados;

- eventuais consequências do tratamento para os titulares; e

- a existência de medidas de proteção (p. ex. pseudonimização/criptografia).

Devido à semelhança das legislações da UE e do Brasil, e considerando a ausência de orientação da Autoridade Nacional de Proteção de Dados brasileira sobre o tema, é possível se utilizar de critérios semelhante aos presentes no teste de compatibilidade europeu no contexto brasileiro.

2.2_Conexão entre as finalidades de uso e inovação

A princípio, pergunta-se, qual deveria ser o grau de conexão entre a nova finalidade e a finalidade inicial de tratamento. Por exemplo, a finalidade de **aprimoramento** de um produto/serviço pode ter uma maior conexão com a finalidade inicial caso o titular venha a ter acesso a essas inovações (p. ex. atualização de um software), do que nos casos em que a inovação está relacionada a **desenvolvimento de novos produtos e serviços** aos quais o titular não necessariamente terá acesso.

Contudo, a partir dos critérios elencados acima observa-se que **o teste de compatibilidade é, em sua essência, uma forma de análise de risco**, e não apenas uma forma estrita de verificação de "compatibilidade" entre finalidades. Desse modo, o teste busca avaliar prioritariamente se a nova finalidade de tratamento dos dados pode ser abusiva, ou colocar o titular em posição de vulnerabilidade. Assim, a verificação da conexão entre a finalidade inicial e posterior, apesar de ser um dos elementos a serem analisados, não seria o critério principal. Ganham maior peso na realização do teste, portanto, os critérios relacionados a verificação dos riscos ao titular dos dados, e a existência de medidas de proteção.

A ênfase na análise de risco em relação à nova finalidade de tratamento está alinhada com a própria essência das legislações de proteção de dados, que se fundamentam na verificação e mitigação prévia de riscos por parte dos agentes (risk-based approach **[2]**). Nesse sentido, o uso posterior para fins de inovação pode ser justificado pelo fundamento do desenvolvimento tecnológico e da inovação previsto na LGPD (art. 2, VI), se o nível de risco estiver adequado. Em outras palavras, um grau de conexão menor entre a nova finalidade (p. ex. inovação) e a finalidade inicial pode ser atenuado, no contexto de uso posterior de dados, desde que o risco do novo tratamento seja baixo e sejam adotados mitigadores de risco.

3_Aplicação de outra base legal

Caso não haja um nível adequado de compatibilidade entre as finalidades, resta ao agente de tratamento verificar se é possível que a nova finalidade seria justificada através de uma nova base legal. Nesse caso ganha destaque a verificação da base legal do legítimo interesse (LI). Apesar de a verificação da base do legítimo interesse ser um tema que merece análise a parte, defende-se que o fundamento da inovação previsto na LGPD (art. 2, V, da LGPD) deve sim ser levado em consideração para análise da legitimidade da nova finalidade de tratamento, no contexto de um teste de LI.

4_Conclusão

Com base no exposto verifica-se que a análise de compatibilidade entre uma finalidade posterior e a finalidade inicial que justificou a coleta de dados não pode ser realizada apenas com base apenas no critério de conexão entre as duas per se. Seja no contexto de aplicação da LGPD ou do GDPR, argumenta-se que **o teste de compatibilidade entre finalidades de uso dos dados** tem como objetivo principal averiguar o nível de risco ao titular que o novo tratamento pode acarretar.

Como as duas legislações de proteção de dados são fundamentadas na noção de verificação prévia e de mitigação de risco (risk-based approach), o teste de compatibilidade entre finalidades de uso dos dados deve também levar em consideração as consequências do novo tratamento para os titulares, e a existência medidas de proteção (p. ex. pseudonimização/criptografia). Dessa forma, uma menor conexão entre as finalidades de tratamento pode ser atenuada desde que o risco da nova finalidade seja baixo ou adequadamente mitigado. Assim, o tratamento posterior de dados pessoais para fins de inovação pode ser adequadamente embasado na LGPD, a depender principalmente das características de risco do caso concreto.

Bibliografia

1- UNIÃO EUROPEIA. Regulation (EU) 2016/679. Disponível em:<https://bit.ly/31FN0ZP>. Acesso em: 09/11/2021.

2- GELLERT, Raphaël. The Risk-Based Approach to Data Protection. Oxford: Oxford University Press, 2020.

03 PEP é um dado pessoal sensível?

PEP é um dado pessoal sensível?

Autor

Lucas Oliveira Balsamão Magela

1_Introdução

É comum em alguns projetos de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), sobretudo de instituições financeiras, se deparar com formulários de declaração de pessoa exposta politicamente (PEP) usados pelo compliance das empresas para gerenciar os seus programas de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP) e à corrupção de seus fornecedores, clientes, parceiros e colaboradores. Nesses casos, por envolver a coleta de diversos dados pessoais, incluindo dados relacionados às questões de cunho político, é comum o questionamento sobre se a declaração de PEP seria ou não classificado como dado pessoal sensível, conforme definição feita na LGPD.

Considerando isso, o objetivo deste texto é abrir um debate sobre esse assunto, tecendo algumas considerações importantes que podem ajudar a prevenir riscos em relação à proteção de dados pessoais tanto para os titulares, que em determinados casos precisam declarar o PEP para ter acesso a serviços e produtos específicos (por exemplo: financeiros), quanto para as empresas, que necessitam dessas informações para os seus programas de PLD/FTP e o cumprimento das obrigações legais aplicáveis.

2_Afinal, o que é PEP e qual o seu objetivo?

O PEP, como conhecemos, é fruto de um esforço regulatório de diversas entidades públicas (com destaque para o Ministério Público, CVM, BACEN e Su-

sep) e da iniciativa de várias empresas e instituições em criar mecanismos para identificar e prevenir crimes de corrupção e lavagem de dinheiros em suas operações.

Os critérios para definir PEP podem variar de acordo com a entidade pública responsável pela regulação. Na maioria dos casos, a definição de PEP é feita por meio de listas que indicam determinados cargos e funções públicas que devem ser considerados no escopo de tal conceito [1]. Outras normas [2], mesmo sendo exceções, trabalham com o conceito de empregos ou funções públicas relevantes.

No entanto, apesar dessas diferenças, no geral, são considerados PEP "os agentes públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou em países estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo" [3].

A partir do PEP, as empresas podem, juntamente com as bases de dados internas e as listas divulgadas em portais da transparência e de bureaus privados, obter as informações necessárias para avaliar os riscos de contratação com esses agentes públicos, o que auxilia na prevenção de possíveis problemas legais, de perda de oportunidades de negócio, de pagamento de multas, além de possíveis danos a sua imagem, marca e reputação.

3_O PEP pode ser classificado como dado pessoal sensível?

Dados pessoais sensíveis, devido a sua própria natureza, têm o potencial de causar mais danos ao titular quando comparados aos demais dados pessoais. Tal ponto se torna especialmente mais problemático quando se observa, por exemplo, o crescente movimento de polarização e intolerância política no Brasil e em diversos países. Dados pessoais sobre opinião ou filiação à organização política, se expostos ou tratados de maneira indevida, podem provocar consequências sérias à integridade psicológica e, inclusive, física do titular. Entender o PEP como um dado sensível não é só uma questão meramente formal da LGPD, mas sim, um conceito importante com consequências práticas que qualquer instituição que trate dados considerados sensíveis precisa observar em sua gestão e governança de privacidade.

A LGPD classifica como dado sensível [4] qualquer "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natura". Nesse sentido, o conceito de PEP, a priori, intercede com a definição de dado sensível ao considerar que é possível obter por meio do PEP informações sobre opinião e filiação a organização política, principalmente quando o agente classificado é ocupante de um cargo eletivo dos Poderes Executivo e Legislativo.

Essa confusão se torna mais acentuada quando se observa o parágrafo 1º do art. 11 da LGPD, que considera sensível quaisquer dados pessoais que revelem dados pessoais sensíveis e que possam causar danos ao titular. Seguindo essa lógica, se o PEP permitir revelar informações sobre a opinião ou a filiação a organização política, é possível concluir que o PEP deve ser classificado como um dado pessoal sensível para fins de aplicação da LGPD. No entanto, essa conclusão não leva em consideração as várias questões práticas aplicáveis ao PEP.

Identificar uma pessoa como PEP ou não ocorre mediante uma declaração específica, geralmente através de marcações em uma lista pré-determinada, onde o próprio titular preenche alguns dados cadastrais (por exemplo: nome, CPF e profissão) e indica se ele se enquadra em alguma das hipóteses consideradas pelas regulações aplicáveis como PEP. Através dessa declaração, as empresas buscam em bases públicas (por exemplo: lista do Portal da Transparência da CGU [5]) e privadas informações adicionais para confirmar se os dados declarados pelo titular são verdadeiros.

Nesses casos, apenas o nome do titular e algumas informações adicionais, como, por exemplo, o cargo e alguns dígitos do CPF, são suficientes para que a empresa tenha as informações necessárias para cumprir com o seu programa de PLD/FTP e de combate à corrupção. Desse modo, muitas declarações de PEP, principalmente quando envolvem agentes públicos, que são considerados PEP, mas que não ocupam cargos eletivos dos poderes Executivos e Legislativo, não geram qualquer tratamento de dados que podem ser considerados sensíveis.

Nesse mesmo sentido, os agentes públicos ocupantes de cargos eletivos dos poderes Executivos e Legislativo, apesar de serem políticos filiados a partidos,

não demandam dos departamentos de compliance, em um primeiro momento e tendo como base as informações presentes na lista divulgada pela CGU, informações adicionais que possam revelar qualquer dado sensível para confirmar se o titular é ou não considerado PEP. Contudo, no caso em que a empresa, por possuir um programa mais robusto de compliance e usa o PEP para obter mais informações que revelem dados que permitem inferir a opinião e filiação política, precisa se ater para o fato de que a declaração de PEP poderá tratar dados considerados sensíveis pela LGPD, conforme, inclusive, entendimento presente no Guia Orientativo no Contexto Eleitoral do TSE e da ANPD [6].

Outra situação que é importante mencionar são os casos de políticos que são figuras notoriamente conhecidas em razão do cargo que ocupam (por exemplo: o governador Doria ou o prefeito da cidade de São Paulo, Ricardo Nunes). Nesses casos, a própria natureza pública do cargo e a sua notoriedade tornam inevitáveis qualquer associação que possa envolver o tratamento de dados sensíveis (por exemplo: é de conhecimento público que o Doria, Lula e Bolsonaro são filiados a um partido político). No entanto, isso não significa necessariamente que a empresa precisa armazenar e tratar essas informações. Desse modo, assim como nos demais casos citados, apenas a simples declaração do titular, validada pela lista pública, já seria suficiente para atingir em grande parte os objetivos legais e o programa interno de PLD/FTP.

Há também os casos que envolvem familiares [7] e estreitos colaboradores [8]. Diferentemente do agente público considerado PEP em razão do seu cargo, a análise dos dados dos estreitos colaboradores e familiares afeta terceiros não ocupantes de cargos públicos, o que exige dos programas de PLD/FTP a coleta de uma quantidade maior de informações e que podem, em determinados contextos e de acordo com o nível de profundidade do programa de compliance da empresa, coletar dados pessoais sensíveis, como, por exemplo, registro de filiação política, para poder de fato avaliar e compreender os riscos de LP/FTP [9] ou corrupção envolvidos na operação.

Portanto, é possível observar que a declaração de PEP, enquanto documento necessário para atingir uma obrigação regulatória ou cumprir com o programa de PLD/FTP, não reuniria por si só as condições necessárias para ser considerado um dado pessoal sensível. Logo, o que vai determinar a qualificação do PEP como dado pessoal sensível dentro do programa de PLD/FTP são as informações adicionais que podem ser obtidas pelas empresas e revelem dados pesso-

ais sensíveis, principalmente dados sobre a filiação e opinião política do titular.

4_Conciliando o PEP e os riscos de PLD/FTP com a LGPD e o papel da ABR nesse processo

Para os casos em que a declaração de PEP é usada pelas empresas para obter dados pessoais adicionais, sejam sensíveis ou não, para cumprir com os seus programas de PLD/FTP e combate à corrupção, é necessário se atentar ao risco do tratamento de dados excessivos ou desnecessários. A solução para isso pode ser encontrada dentro dos próprios conceitos de gestão de risco dos programas de PLD/FTP.

Para evitar possíveis casos de falsos positivos, erros, processos lentos e burocrático nos programas de PLD/FTP, desenvolveu-se o conceito de Abordagem Baseada em Risco (ABR), inclusive já adotado em regulações de compliance. A função da ABR é orientar o compliance das empresas a implementar medidas de identificação, avaliação, monitoramento, gestão e mitigação de riscos de LD/FTP de modo dinâmico e proporcional ao risco envolvido. Desse modo, quando os riscos forem considerados menores, devem ser adotadas medidas mais simples e céleres. Por outro lado, quando os riscos forem mais significativos, medidas mais robustas e que demandem mais tempo deverão ser usadas para prevenir corrupção, lavagem de dinheiro ou de financiamento ao terrorismo nas operações.

Nesse sentido, a ABR, que trabalha diretamente com conceito de avaliação de risco, pode servir de base para uma gestão dos dados pessoais tratados dentro de um programa eficiente de PLD/FTP. No caso, a ABR poderia incorporar na avaliação os riscos relacionados ao tratamento de dados pessoais. A partir disso, os casos de menor risco, por exemplo, deverão evitar a coleta de dados adicionais que não são necessários para uma gestão eficiente do PLD/FTP. Já nos casos de risco iminente de LD/FTP, a coleta de dados pessoais adicionais, até mesmo dados pessoais sensíveis, obtidos através do PEP e de outras bases de dados públicos e privados, é justificável para reunir todas as informações indispensáveis para cumprir com o programa de PLD/FTP e as obrigações legais aplicáveis.

5_Conclusão

Conforme vimos, o PEP por si só não é capaz de revelar dados sensíveis do titular, contudo, quando observado dentro de um programa de PLD/FTP, o PEP poderá ser usado como base para revelar informações sensíveis do seu titular, dos seus familiares ou colaboradores estreitos. Nesses casos, a implementação de uma ABR, que seja capaz de determinar a necessidade da coleta de dados adicionais para cumprir as obrigações de PLD/FTP, é fundamental para prevenir o tratamento de dados pessoais, inclusive sensíveis, que em determinados contextos serão desnecessários e prejudiciais para toda a governança de dados pessoais das empresas.

Bibliografia

1- Art. 1º, do Anexo A, da Resolução CVM nº 50, de 31 de agosto de 2021.

2- Art. 4º, da Circular Susep nº 612, de 18 de agosto de 2020.

3- Art. 5º, do Anexo A da Resolução CVM nº 50, de 31 de agosto de 2021.

4- Inciso II, do art. 5º, da Lei nº 13.709, de 14 de agosto de 2018.

5- Nessa lista é possível encontrar parte do CPF, nome completo, sigla da função, descrição da função, nível da função, nome do órgão público, data de início, data de término e prazo final da carência. Disponível em: <http://www.portaldatransparencia.gov.br/download-de-dados/pep>. Acesso em: 15/10/2021.

6- Brasil. Autoridade Nacional de Proteção de Dados e Tribunal Superior Eleitoral. Guia Orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral. TSE. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf >. Acessado em: 19/01/2022.

7- Inciso I, do art. 6º, do Anexo A da Resolução CVM nº 50, de 31 de agosto de 2021.

8- Inciso II, do art. 6º, do Anexo A da Resolução CVM nº 50, de 31 de agosto de 2021.

9- Quando sem o "P" significa "lavagem de dinheiro e financiamento ao terrorismo e à proliferação de armas de destruição em massa.

10- CARVALHO, Andre Castro. Pessoa politicamente exposta: reflexões e propostas de regulamentação. Consultor Jurídico. 2021. Disponível em: <https://www.conjur.com.br/2021-set-19/publico-pragmatico-pessoa-politicamente-exposta-reflexoes-propostas-regulamentacao#_ftn2>. Acessado em: 15/10/2021.

04 Norma administrativa chinesa regula algoritmos de recomendação de conteúdo

Voltar para o índice

Norma administrativa chinesa regula algoritmos de recomendação de conteúdo

Autores

Luiz Felipe Sundfeld Ibrahim

Odélio Porto Júnior

1_Introdução

A facilidade de se coletar dados pessoais de usuários no contexto de serviços disponibilizados na internet tem permitido um maior desenvolvimento de algoritmos de recomendação, os quais podem se basear nas características individuais inferidas dos dados dos usuários (por exemplo, recomendação de conteúdo ou de serviços e produtos, algoritmos de busca e filtragem de conteúdo, entre outros). Nesse contexto, no dia 27 de agosto de 2021, a Administração do Ciberespaço da China (ACC)[1] – órgão regulador da internet chinesa – tornou pública para consulta uma minuta de norma administrativa que visa regulamentar o uso de algoritmos de recomendação no país.[2] Em 04 de janeiro de 2022, a ACC anunciou que a norma entrará em vigor em março de 2022.[3] Este texto busca analisar de forma geral o conteúdo da regulamentação chinesa.[4]

[1]Em inglês "the Cyberspace Administration of China" (CAC).

[2]TONER, Helen; CREEMERS, Rogier; e WEBSTER, Graham. Translation: Internet Information Service Algorithmic Recommendation Management Provisions (Draft for Comment). Agosto de 2021. Disponível em: <https://stanford.io/3HMaVau>. Acesso em: 22/11/2021.

[3]THE STATE COUNCIL THE PEOPLE'S REPUBLIC OF CHINA. China to implement new regulation on algorithm recommendation services. 2022. Disponível em: < https://english.www.gov.cn/news/topnews/202201/04/content_WS61d3f8fbc6d09c94e48a31d1.html>.

[4]A análise do conteúdo da norma foi feita com base na tradução para o inglês da minuta publicada em agosto de 2021 (ver noda de rodapé nº 3).

2_O que diz a norma

A proposta de norma possui 30 artigos, tendo um caráter marcadamente principiológico. Por exemplo, é vedado o uso de algoritmos de recomendação que possam violar direitos dos cidadãos, violar o interesse público ou a segurança nacional chinesa, que incentivem o vício e o alto consumo, bem como algoritmos que promovam atividades que possam colocar em perigo a ordem social ou econômica da China.

De forma geral, os principais temas regulados são os seguintes:

• Obrigação de transparência com os usuários, devendo ser fornecidas informações básicas sobre o funcionamento do algoritmo;

• Dar aos usuários a opção de desativar recomendações baseadas em suas características individuais;

• Dever de testar periodicamente os algoritmos, para verificar que eles não estão induzindo os usuários a práticas danosas ou ilícitas (por exemplo, gastos excessivos, atividades que prejudicam a saúde mental das pessoas ou a ordem econômica do país, entre outros);

• Proibição do uso de algoritmos de recomendação para tratamento diferenciado ilícito de consumidores (por exemplo, preços distintos entre indivíduos com base em suas características);

• Resguardar os indivíduos menores de idade de conteúdos digitais prejudiciais à saúde mental e física, evitando o aumento de jovens viciados em tecnologias;

• Proteções específicas para idosos;[5]

• Especificamente para empresas que possuem a capacidade de afetar a segurança nacional ou influenciar a opinião pública chinesa, a minuta propõe que o algoritmo seja previamente submetido à aprovação dos órgãos reguladores chineses, sob pena de sanção (por exemplo, proibição da prestação dos serviços e multa); e

[5] ONETRUST DATAGUIDANCE. China: CAC issues Internet Information Service Algorithm Recommendation Management Regulations. 2022. Disponível em: <https://www.dataguidance.com/news/china-cac-issues-internet-information-service-algorithm>.

• No caso de algoritmos usados em plataformas para intermediação de oferta de trabalho a prestadores de serviço (por exemplo, transporte privado de passageiros e serviços de entregas), a empresa deve fornecer informações sobre cálculo da remuneração do usuário, tempo de trabalho, entre outras informações.

Importante destacar que a norma se aplica apenas a entidades privadas que utilizem algoritmos de recomendação na disponibilização de serviços de internet.

3_Pontos de destaque

3.1_Transparência e Direito à explicação

Utilizando lógica semelhante ao direito à explicação de decisões automatizadas previsto no GDPR e na LGPD, a norma administrativa chinesa também prevê a obrigação de as empresas serem transparentes em relação a como os algoritmos funcionam (artigo 12). O texto da minuta impõe que as empresas devem publicizar "os princípios, finalidades, motivos e mecanismos operacionais dos algoritmos" (artigo 14). Contudo, a norma não chega a inovar em relação a como enfrentar as dificuldades técnicas de se explicar o funcionamento de algoritmos de inteligência artificial, problema conhecido como "black box", o qual tem sido amplamente discutido na União Europeia e nos Estados Unidos.[6]

3.2_Personalização do algoritmo pelo usuário

A minuta busca conceder ao usuário maior autonomia em relação a como ele pode ser afetado por um algoritmo de recomendação. Além de conceder ao usuário o direito de ter informações sobre o funcionamento do algoritmo e o de optar por não receber recomendações personalizadas (opt-out), a regulação impõe que as empresas disponibilizem funcionalidades para que os próprios usuários possam escolher quais critérios o algoritmo irá utilizar para a apresentação das recomendações (artigo 15). Apesar de não entrar em detalhes, a norma explica que as categorias de conteúdo (tags) utilizadas pelo al-

[6]SELBST, Andrew; POWLES, Julia. "Meaningful Information" and the Right to Explanation. International Data Privacy Law, vol. 7(4). 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125>.

goritmo devem poder ser visualizadas e editadas pelos próprios usuários. A pesquisadora da Universidade de Georgetown (EUA) Helen Toner aponta que esta medida, apesar de interessante, pode ser uma simplificação que não abarca o verdadeiro funcionamento de um algoritmo de recomendação, o qual, em realidade, utiliza uma série de fatores e correlações de natureza complexa que são de difícil compreensão até para especialistas.[7] Toner aponta, ainda, que atribuir apenas ao usuário a responsabilidade pela verificação dos algoritmos pode ser inviável na prática em certa medida, considerando a complexidade dos algoritmos.

4_Conclusão

A norma administrativa apresenta como elementos centrais a tentativa de proteção dos indivíduos afetados por algoritmos de recomendação, principalmente sob o viés consumerista e trabalhista, e busca reforçar o controle pelo governo chinês do conteúdo disponibilizado na internet.

Considerando a realidade brasileira, é interessante acompanhar como se dará a aplicação dessa norma em relação à busca de uma maior transparência para com os usuários sobre como os algoritmos de recomendação funcionam e os afetam, principalmente em relação às searas trabalhistas, consumerista e de proteção de dados pessoais.

[7] TONER, Helen; PAUL, Triolo; e CREEMERS, Rogiers. Experts Examine China's Pioneering Draft Algorithm Regulations. 2021. Disponível em: <https://digichina.stanford.edu/work/experts-examine-chinas-pioneering-draft-algorithm-regulations/>.

05 Serviços baseados em nuvem: novos desafios regulatórios para contratação

Voltar para o índice

Serviços baseados em nuvem: novos desafios regulatórios para contratação

Autores:

Matheus Botsman Kasputis.

Odélio Porto Júnior.

1_Introdução

Pesquisas indicam que, hoje, 81% das empresas utilizam dois ou mais serviços diferentes de computação em nuvem (cloud computing) em seus negócios.[1] A adesão aos regimes de home office no meio corporativo vem contribuindo, ainda mais, para a penetração desse tipo de tecnologia na atividade empresarial. Tais serviços podem ser providos em diversas formas, incluindo infraestrutura, software e plataformas, adaptando-se aos vários modelos de negócio.

Os serviços baseados na nuvem beneficiam, principalmente, os pequenos e médios negócios, trazendo preços competitivos e vantagens operacionais. O armazenamento de dados em nuvem, por exemplo, reduz custos e incentiva a digitalização de processos. Ao mesmo tempo, permite o acesso e a edição compartilhada desses arquivos, sob demanda, mediante conexão com a internet.

Por outro lado, os serviços em nuvem podem trazer riscos de proteção de dados pessoais. Considerando a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, e a Autoridade Nacional de Proteção de Dados (ANPD), o setor privado deverá assumir certos cuidados na contratação desses serviços.

[1]NOTT, Chris. Cloud Portability and interoperability. 20 de outubro de 2020. Disponível em < https://www.ibm.com/blogs/think/fi-fi/2020/10/20/cloud-portability-and-interoperability/>. Acesso em 25.10.2021.

Como os serviços em nuvem são regulados pelas leis de proteção de dados?

Atualmente, não há regulamentação específica sobre serviços em nuvem no Brasil. No entanto, as regras de proteção de dados aplicam-se diretamente a esses serviços quando utilizados como meios para o tratamento de dados pessoais, o que inclui qualquer acesso, visualização ou armazenamento de informações que identifiquem ou possam identificar alguém.

Destacamos abaixo quatro principais aspectos que são regulados pela legislação brasileira na contratação desses serviços.

2_A responsabilidade entre os agentes

A ANPD já deixou claro que os provedores de serviços em nuvem, quando contratados para essa finalidade, são operadores dos dados pessoais.[2] Os contratantes, por terem poder decisório sobre o tratamento das informações, são controladores dos dados e, por isso, podem ser responsabilizados pelos danos causados aos titulares (p. ex. colaboradores, clientes e representantes de parceiros ou fornecedores) pelo provedor do serviço de nuvem.

Isso significa que havendo vazamento do servidor em que os dados são hospedados, por exemplo, o consumidor poderá acionar judicialmente tanto a empresa com a qual mantém relação quanto o provedor do serviço em nuvem, a fim de buscar reparação. A princípio, a empresa pode alegar uma excludente de responsabilidade, como culpa exclusiva do provedor de serviços, para evitar ser responsabilizada solidariamente. Contudo, essa alegação pode ser de difícil sustentação, principalmente quando os afetados forem consumidores (responsabilidade objetiva prevista no CDC), e quando se considera que a responsabilização pelo tratamento de dados na LGPD é predominantemente do controlador dos dados.

A relação pode se tornar ainda mais complexa quando envolver terceiros. Fornecedores da empresa, por exemplo, podem subcontratar provedores de ser-

[2]ANPD. Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Maio de 2021, versão 1.0. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em 26.10.2021.

viço em nuvem, hipótese em que haverá um suboperador no tratamento dos dados. Em outro caso, também, a empresa pode acessar e editar arquivos junto a um parceiro de negócio, situação em que pode haver controladoria conjunta dos dados. Tais situações mais complexas devem ser analisadas com cuidado para fins de prestação de contas ao titular e aos órgãos reguladores.

3_ As relações de transparência

A LGPD estabelece uma série de obrigações de transparência que devem ser observadas por aqueles que tratam dados pessoais. No que toca aos serviços em nuvem, os contratantes devem informar os titulares, especialmente, sobre a forma, duração e finalidade específica do tratamento dos dados. Também deverão esclarecer que haverá compartilhamento de determinadas informações sobre o titular com provedores de serviços em nuvem.

A lei e a regulação ainda não determinaram qual deve ser o nível de detalhamento em relação ao dever de informar o titular sobre o compartilhamento de seus dados, de modo que se recomenda que o controlador informe, ao menos, que realiza o compartilhamento com essa categoria de fornecedores (serviços de cloud).

4_As obrigações de segurança da informação

Quando da contratação de serviços em nuvem, é importante observância às regras de governança e segurança da informação da LGPD, visando a garantia da proteção dos dados pessoais. Nesse sentido, é importante verificar se o fornecedor possui certificações de segurança específicas para serviços de nuvem (p. ex. SOC 2; ISO 27001; CSA STAR).

Os diferenciais competitivos de muitos provedores de serviços em nuvem encontram-se justamente na infraestrutura de segurança oferecida, que pode garantir controles de versão de arquivos, criptografia, antimalware, ferramentas de controles de acesso, entre outras medidas que exigiriam alto custo para serem atingidas em servidores on-premisse. Diante disso, tais aspectos

devem assumir prioridade nas negociações e na escolha dos provedores de serviços em nuvem.

5_A transferência internacional de dados

Atualmente, alguns planos de serviços em nuvem disponibilizam, apenas, a opção de contratar servidores localizados fora do Brasil. A escolha por servidores em território estrangeiro implica maiores obrigações aos contratantes, uma vez que as leis nacionais e estrangeiras de proteção de dados impõem, por vezes, requisitos adicionais para casos de transferência internacional.

A LGPD, por exemplo, exige a implementação de mecanismos aptos a legitimar tais transferências internacionais, que podem incluir cláusulas padrão, decisões de adequação pela ANPD sobre o país de destino dos dados, a existência de códigos de conduta e certificados sobre proteção de dados, ou, ainda, a obtenção de um consentimento específico do titular para a transferência, ou a existência de um contrato prévio com o titular.

Por outro lado, devido à variedade de produtos disponíveis no estrangeiro, as transferências internacionais podem ser contrapesos atrativos pelo potencial de garantir mais proteção aos dados compartilhados, seja pela incidência de leis mais rigorosas, pelo estado de arte da tecnologia no país destinatário ou pelas medidas de segurança oferecidas pelos provedores.

Quais cuidados devem ser considerados na contratação?

Diante dos aspectos mencionados acima, recomenda-se aos contratantes a adoção de uma série de cuidados nas negociações de serviços em nuvem.

Deve-se ter por claro, em primeiro lugar, qual tipo de serviço em nuvem será contratado (infraestrutura, software ou plataforma), quais tipos de dados serão compartilhados, e para quais finalidades serão tratados. O contratante deverá buscar os fornecedores mais adequados a esses objetivos e em conformidade às leis de proteção de dados.

Na sequência, recomenda-se a condução de um **due diligence** dos fornecedores selecionados, com o enfoque em aspectos de proteção de dados, que pode

abranger um mapeamento dos seguintes tópicos:

• certificados e medidas de segurança adotadas pelo provedor do serviço, com destaque para a criptografia;

• as medidas de prestação de contas viabilizadas pelo serviço, incluindo controle de versões/acesso aos arquivos armazenados;

• os aspectos de retenção e descarte dos dados pessoais armazenados, incluindo backups dos arquivos;

• a facilidade na gestão e no exercício dos direitos dos titulares, como a portabilidade de dados por mecanismos de exportação ou solicitação de acesso;

• a personalização dos níveis de acesso aos dados armazenados, incluindo o acesso/compartilhamento a terceiros; e

• a localização dos servidores para fins de transferência internacional dos dados armazenados.

Mapeados esses aspectos e selecionado o provedor do serviço, é importante que seja celebrado um **acordo de nível de serviço** (service level agreement – SLA) entre as partes a fim de formalizar a relação jurídica. Esse acordo deve deliberar sobre todos os aspectos mencionados anteriormente, com destaque para: a finalidade do tratamento dos dados, as responsabilidades das partes, as medidas de segurança empregadas, as medidas de transparência adotadas, os mecanismos de transferência internacional utilizados, as bases legais válidas, o período de retenção e descarte dos dados, entre outros aspectos.

É importante observar que alguns fornecedores, normalmente grandes players do mercado, costumam já ter um SLA padrão, limitando a negociabilidade desses acordos por meio de contratos de adesão. Essas práticas também devem ser analisadas a fim de se decidir ou não pela contratação, de acordo com as condições do acordo oferecido e os riscos jurídicos.

A depender do porte do contratante e/ou dos dados pessoais tratados as condições acordadas podem ser mais ou menos rigorosas. A LGPD, por exemplo, estabelece tratamento diferenciado para as microempresas, empresas de pequeno porte e startups, principalmente quanto às medidas de segurança da

informação exigidas. A ANPD, em guia orientativo sobre a matéria[4], recomenda que essas empresas, ao contratarem serviços em nuvem:

- verifiquem a observância do provedor às recomendações internacionais e boas práticas de segurança da informação;

- celebrem um acordo de nível de serviço com o provedor, disciplinando a segurança dos dados armazenados; e

- especifiquem os requisitos de acesso para cada tipo de serviço utilizado, e apliquem técnicas de autenticação multifator (como SMS ou aplicativos autenticadores).

E depois – quais são os próximos passos?

A contratação do serviço em nuvem não encerra as obrigações do contratante. É necessário, ainda, o monitoramento e auditoria constante do provedor do serviço a fim de assegurar-se que os mesmos níveis protetivos são mantidos, evitando futuro risco de responsabilização.

Além disso, mostra-se fundamental treinar e educar os colaboradores à utilização consciente e adequada das ferramentas disponibilizadas pelo provedor, aplicando, inclusive, as políticas e os procedimentos internos da empresa visando a assegurar o seu correto uso.

Os serviços em nuvem são, portanto, ferramentas poderosas que podem contribuir para a proteção de dados pessoais do contratante, mas precisam possuir uma estrutura robusta de governança de dados.

[3]ANPD. Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Outubro de 2021, versão 1.0. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em 26.10.2021.

BAPTISTA LUZ
ADVOGADOS

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br