Impactos da Lei Geral de Proteção de Dados nas *Health Techs*

Health Techs podem ser resumidas em três grandes blocos de atuação, sendo prevenção, tratamento e diagnóstico. São modelos de negócio escaláveis e inovadores que permitem agir de forma **preventiva, preditiva, proativa e personalizada.**

Nesse setor, os investimentos realizados no primeiro semestre de 2021 atingiram US$ 91,7 milhões, representando 85% do que foi acumulado ao longo de 2020, de acordo com levantamento do Distrito. O mercado das *Health Techs* no Brasil tem quase 700 startups concentradas majoritariamente na região Sudeste, empregando mais de 10 mil pessoas. A maioria está em fase inicial, várias impulsionadas pela criação de *hubs* para ajudar no desenvolvimento de tais empresas, como o recente *Hub* de Inovação do Hospital do Amor de Barretos, SP.

Como está a regulamentação sobre proteção de dados lá fora?

Atualmente, segundo levantamento da *United Nation Conference on Trade and Development* (UNCTAD), cerca de 66% dos países possuem leis sobre proteção de dados pessoais e 10% dos países em fase de elaboração de regulamentação sobre o tema[1].

No âmbito da União Europeia, destaca-se o **Regulamento Geral sobre Proteção de Dados** (GDPR). Destaca-se que o setor da saúde foi um dos mais multados por descumprimento do Regulamento nos últimos anos[2].

Já os **Estados Unidos não contam com uma "lei geral" sobre a matéria,** mas leis estaduais esparsas.

Especificamente sobre a regulamentação de dados de saúde, destaca-se a *Health Insurance Portability and Accountability Act* (**HIPAA**)[3] de 1996, contendo dispositivos quanto à proteção, utilização, armazenamento e qualidade dos dados de saúde quando manuseadas por entes específicos.

Em 2009, para complementar a HIPPA, foi elaborada a **HITECH Act**[4], no tocante à implementação de um programa de compliance, modernização dos registros médicos e a inclusão de sanções monetárias significativas. Ainda, pode ocorrer a aplicação das disposições do *Federal Food, Drug and Cosmetic Act, Federal Trade Comission Act e FTC's Health Breach Notification Rule*[5].

---

[1] UNCTAD. Data Protection and Privacy Legislation Worldwide. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[2] Disponível em: https://www.enforcementtracker.com/.

[3] U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. Summary of the HIPAA Privacy Rule. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[4] U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. HITECH Act Enforcement Interim Final Rule. Disponível em: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

[5] OFT. Developing a mobile healt app? Disponponível em: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

No Brasil, o que é a LGPD?

Considerando o movimento internacional e a necessidade de criação de ferramentas para proteção dos titulares de dados pessoais, foi promulgada a Lei no 13.709 em agosto de 2018, conhecida como **Lei Geral de Proteção de Dados Pessoais** (LGPD).

Ao longo de seus 65 artigos, se encarrega de trazer definições que norteiam a matéria, os requisitos para tratamentos de dados pessoais e seus agentes, transferência internacional, princípios, direitos dos titulares, a criação da **Autoridade Nacional de Proteção de Dados** (ANPD), de um **Conselho Nacional de Proteção de Dados Pessoais e Privacidade** e sanções administrativas em caso de descumprimento da lei.

O que são dados de saúde?

Dados pessoais são informações relacionadas a uma pessoa natural **identificada ou identificável.**

A LGPD qualifica o dado pessoal referente à saúde como dado pessoal sensível, conferindo uma proteção especial em comparação aos demais. Dados sensíveis têm maior potencial de discriminação do indivíduo e possuem uma proteção especial.

Portanto, dados pessoais de saúde podem compreender desde prontuários médicos, fichas de funcionários, até dados que, pelo contexto, podem se referir à saúde do titular, como quantidade de passos, horas dormidas, nível de estresse, alimentação, entre outros.

Estes dados, além de observar todos os princípios da LGPD, têm requisitos específicos de tratamento e vedação quanto ao compartilhamento entre controladores com o intuito de obter vantagem econômica, salvo exceções do artigo 11, parágrafo 4º da lei.

Nesse contexto, destaca-se a alteração legislativa conferida pela Medida Provisória 869/2018, convertida na **Lei no 13.853/2019**. Tal lei trata do setor de saúde, planos privados, assistência farmacêutica e de assistência à saúde, que permite a portabilidade de dados entre controladores em benefício aos interesses do titular, bem como a **proibição** quanto ao uso desses dados na contratação, seleção de risco ou até a exclusão de beneficiários por operadoras de planos de saúde privados.

Sob qual justificativa posso tratar dados sensíveis?

De acordo com a LGPD, para que seja realizado qualquer tratamento de dados pessoais sensíveis, seja o acesso, a modificação, o cadastro, a coleta, o descarte, entre outros, é necessário que seja observada uma das bases legais previstas no artigo 11, agrupadas em dois grupos:

Com consentimento	Sem consentimento
• Desde que a manifestação seja livre, inequívoca, informada, **específica e destacada.**	• Cumprimento de **obrigação** legal ou regulatória pelo controlador; • Execução de **políticas** públicas pela administração pública; • Estudos por órgãos de **pesquisa**; • **Exercício regular** de direitos em processos judicial, administrativo e arbitral; • Proteção da **vida ou incolumidade física** do titular ou terceiro; • Tutela da **saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou • Garantia de **prevenção à fraude e segurança** do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Portanto, quando a base legal for a tutela da saúde, a operação de tratamento deve ser realizada apenas por profissionais da área, serviços de saúde ou autoridades sanitárias.

Ademais, a LGPD impossibilita o tratamento de dados pessoais sensíveis com fundamento no legítimo interesse.

O que acontece se eu não seguir a lei?

A função de fiscalização e observância do cumprimento integral da LGPD é de responsabilidade da ANPD, recentemente estruturada. A apuração da infração é verificada mediante instauração de processo administrativo com contraditório e ampla defesa. As sanções que podem ser aplicadas a partir de agosto de 2021 são:

- Advertência, com orientações quanto a medidas corretivas;
- Multas de até 2% do faturamento anual limitada a 50 milhões por infração;
- Publicização da infração;
- Bloqueio dos dados pessoais até regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados;
- Suspensão ou proibição (parcial ou total) de atividade relacionada.

Razoavelmente, a própria lei estabelece que a sanção deve ser proporcional ao dano causado e observar critérios, como reincidência, grau de dano, cooperação, boa-fé do infrator. Assim, é provável que infrações que envolvam dados pessoais sensíveis atrairão **sanções mais graves**. Além de tais sanções, já é possível a propositura de ações judiciais com base na lei, sem prejuízo de medidas impostas por outras autoridades, como Secretaria Nacional do Consumidor, que já firmou Acordo de Cooperação Técnica com a ANPD.

Vazaram dados, e agora?

Regulamentação não é sinônimo de conformidade das empresas ou ausência de incidentes de segurança. Tais incidentes abrangem não apenas vazamentos, mas perda de dados, acesso sem autorização, entre outros, cada vez mais frequentes em todo o mundo.

Segundo levantamento da ONG *Privacy International*, aplicativos populares de monitoramento de ciclos menstruais coletaram dados de saúde em desacordo com o GDPR[6]. Ainda, tais dados eram compartilhados com terceiros para fins comerciais, como publicidade.

Do território norte-americano, *New York State Departament of Finnancial Services* elaborou um relatório após notícias de compartilhamento irregular de dados pessoais de saúde de aplicativos de controle menstrual com o Facebook[7]. Como resultado, foi noticiado que o Facebook implementou sistema para identificação e bloqueio de dados considerados sensíveis, que inclui uma lista de 70 mil termos, incluindo os de saúde.

No Brasil, no início do ano de 2021, foi revelado um vazamento de dados pessoais de 223 milhões de pessoas, cuja origem ainda não foi apurada[8]. Especificamente ao setor de saúde, foi noticiado incidente de segurança envolvendo falha no sistema do Ministério da Saúde que expôs os dados de mais de 200 milhões de brasileiros com cadastro no Sistema Único de Saúde (SUS) e planos privados[9].

> *Em novembro de 2020, ocorreu vazamento de dados sensíveis de 16 milhões de brasileiros quanto aos diagnósticos de Covid-19 e doenças pré-existentes, em razão publicação de planilhas que continham senhas de sistemas do Ministério da Saúde, utilizadas em parceria com hospital de renome[10].*

[6] NADAL, M. VICTORIA S. Apps de controle menstrual coletam dados íntimos e os compartilham com Amazon, Google e Facebook. El País, 04. jan. 2021. Disponível em: https://brasil.elpais.com/tecnologia/2021-01-04/apps-de-controle-menstrual-coletam-dados-intimos-e-os-compartilham-com-amazon-google-e-facebook.html.

[7] NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES. Governor Cuomo Accepts Report From Dfs On Facebook Investigation. 18 fev. 2021. Disponível em: https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202102182.

[8] G1. Vazamento de dados de 223 milhões de brasileiros. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml.

[9] INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Vazamentos de dados de saúde coloca consumidor em risco; veja o que fazer. IDEC, 02 dez. 2020. Disponível em: https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer.

[10] G1. Vazamento de senhas do Ministério da Saúde expõe informações de pacientes de Covid-19, diz jornal. G1, 26 nov. 2020. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml.

Todos os agentes de tratamento de dados estão sujeitos a incidentes. O importante é que estejam preparados para responder ao ocorrido, com um plano de resposta estruturado, bem como mitigar os danos causados, resguardando os titulares.

Health Techs devem lembrar de algo mais?

Além dos itens trazidos acima, *health techs* devem se atentar a outros, como:

- Normas setoriais;
- Compartilhamento de dados pessoais entre controladores.
  - » Por exemplo, é proibida a **venda de bases de dados** quando desrespeita a finalidade informada ao titular e os princípios previstos na LGPD. Da mesma forma, **programas de descontos** em farmácias após coleta de CPFs devem respeitar princípios da transparência e finalidade;
- Autoridades competentes como Agência Nacional de Saúde Suplementar, Autoridade Nacional de Vigilância Sanitária, Ministério da Saúde, Conselho Federal de Medicina, Conselho Federal de Enfermagem, entre outros conselhos profissionais, e suas normativas sobre variados temas, como prontuário eletrônico do paciente, padrão de troca de informações, dever de sigilo, obrigações de determinadas empresas etc.;
- Padrões de segurança no desenvolvimento de softwares.
  - » Nesse contexto, a ANVISA publicou o Guia 38/2020 sobre Princípios e Práticas de Cibersegurança em Dispositivos Médicos[11] visando equilibrar a segurança do usuário e do dispositivo incorporando controles de cibersegurança e mitigação de riscos.

Privacy by design, qual o benefício?

Startups, como *health techs*, têm a vantagem de estarem se estruturando ou de ter uma estrutura e operação recentes, o que facilita a adequação à LGPD.

Isso porque, desde o início, **se torna possível prevenir danos e incorporar a privacidade ao projeto**, além de implementar outros princípios do *privacy by design* como segurança de ponta a ponta, visibilidade e transparência, respeito pela privacidade do usuário e funcionalidade total.

---

[11] ANVISA. Guia 38/2020. Princípios e Práticas de Cibersegurança em Dispositivos Médicos. Versão 1. Set. 2020. Brasil. Disponível em: https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2020/saiba-mais-sobre-ciberseguranca-em-dispositivos-medicos/guia-38.pdf.

Na prática, o que tudo isso significa?

Para a conformidade com a LGPD, são essenciais algumas medidas imediatas pelas empresas e health techs.

- As operações de tratamento, cujo **registro** precisa estar atualizado, devem respeitar os **princípios** da lei, entre eles, o princípio da necessidade, com a minimização dos dados tratados, evitando-se dados excessivos, desnecessários ou incorretos.
- Os **contratos** devem ser revistos e explicitarem a finalidade do tratamento e especificidades que envolvem dados sensíveis.
- Contratos com terceiros devem delimitar a **responsabilidade** da empresa.
- O legítimo interesse, como base legal, não deve ser utilizado para dados sensíveis.
- Empresas, incluindo as *health techs*, devem se atentar aos dados de saúde de seus **funcionários**.
- Existência de **políticas de retenção e descarte** de dados.
- Havendo scores de saúde e formação de perfis, recomenda-se a realização de um **relatório de impacto à proteção de dados** para analisar os riscos envolvidos e as medidas de salvaguardas possíveis.
- Ocorrência de **treinamento periódico** de funcionários.
- Estabelecimento de **procedimentos e canais de atendimento** para efetivação de direitos dos titulares como direito à oposição, eliminação, revogação de consentimento, acesso, retificação de dados, revisão de decisões automatizadas etc.).
- **Políticas de privacidade** externa e interna devem ser claras, revisadas periodicamente e disponíveis a todos os interessados.
- Deve existir uma **política de segurança da informação e medidas preventivas** que evitem incidentes de segurança. Por esse motivo, recomenda-se criptografia e anonimização, quando possíveis.

Contatos

Flavia Mansur Murad Schaal

fmm@muradpma.com

Doutora em Direito da Propriedade Intelectual pela Universidade Lorraine, França, revalidado pela UNB – Universidade de Brasília. Mestre em Droit des Affaires Internationales, pela Universidade René Descartes.

Diplomada pelo Franklin Pierce Law Center, em Propriedade Intelectual, e pelo Programa em Direção Geral (Program for Management Development – PMD) – ISE Business School – IESE Universidade de Navarra.

Coordenadora do núcleo de Propriedade Intelectual e digital do CEU LAW SCHOOL. Professora dos cursos de pós-graduação em Fashion Law, da Faculdade Santa Marcelina, do curso de formação em Propriedade Industrial, da Associação Brasileira dos Agentes da Propriedade Industrial, professora do International Trademark Course – South America, Central America and Mexico Panel da INTA – International Trademark Association. Além de mediadora formada pelo Centro de Solução de Disputas em Propriedade Intelectual, CSD ABPI, Brasil.

Pietra Daneluzzi Quinelato

pdq@muradpma.com

Mestranda e Bacharel em Direito pela Universidade de São Paulo. Especialista em Direito Digital e Proteção de Dados pela ESA-SP e Escola Brasileira de Direito. Pós-graduanda em Direito Empresarial pelo CEU Law School.

Certificada como Data Protection Officer pela EXIN. Membro das Comissões de Direito Digital, Direito da Moda e Privacidade e Proteção de Dados da OAB/SP. Pesquisadora dos grupos Sociedade em Rede, Concorrência e Inovação e Direito da Moda da Universidade de São Paulo e da Comunidade Internacional de Estudos em Direito Digital da Universidade Federal de Uberlândia.

Professora convidada do Trilhante em Proteção de Dados Pessoais e Fashion Law. Advogada atuante em inovação, propriedade intelectual e proteção de dados. Autora de artigos em periódicos e livros em proteção de dados e economia digital.