LEI GERAL DE PROTEÇÃO DE DADOS APLICADA À SAÚDE

GENERAL DATA PROTECTION LAW APPLIED TO HEALTH

Jeferson Morais da Costa [1]
Stefan de Oliveira Rosa [2]

Resumo: *A elaboração da Lei Geral de Proteção de Dados levou 8 anos para chegar à sua fase final. Foi finalmente aprovado em 2019 e passou a vigorar em 2020, portanto ainda está em processo de adaptação em muitos dos seus artigos. Quando a LGPD é aplicada à saúde muitos questionamentos se veem surgir. Este trabalho tem por objetivo estudar a LGPD aplicada à área da saúde. Sabe-se que no âmbito da saúde, o prontuário é ferramenta essencial para profissionais da saúde, uma vez que contém todo o histórico de saúde do paciente. Diante disso, o que muda no tratamento do prontuário pela equipe médica?*
Palavras-chave: *Saúde. Direito. Informação.*

Abstract: *The elaboration of the General Law of Data Protection took 8 years to reach its final phase. It was finally passed in 2019 and took effect in 2020, so it is still in the process of adaptation in many of its articles. When LGPD is applied to health many questions arise. This work aims to study LGPD applied to the health area. It is known that in the health field, the chart is an essential tool for health professionals, since it contains all the patient's health history. Therefore, what changes in the medical team's treatment of the medical chart?*
Keywords: *Health. Law. Information.*

[1] Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação pela Universidade Federal do Tocantins (UFT). Professor do Curso de Sistemas de Informação do IFTO.
Lattes: http://lattes.cnpq.br/8929854109676237.
ORCID: https://orcid.org/0000-0001-7605-3174.
E-mail: jeferson.costa@ifto.edu.br.

[2] Mestre em Computação Aplicada pela Universidade do Vale do Rio dos Sinos (Unisinos). Professor do Curso de Sistemas de Informação do IFTO.
Lattes: http://lattes.cnpq.br/2774705785638791.
ORCID: https://orcid.org/0000-0002-6966-5153.
E-mail: stefan@ifto.edu.br.

Introdução

O gratuito tem grande poder de influência na vida dos seres humanos, especialmente para a cultura brasileira tão acostumada a alcançar os objetivos sem muito esforço. Com a premissa da gratuidade, o mundo viu surgir a *World Wide Web*. Com efeito, incialmente o que mais impulsionou o aumento da rede em escala global fora exatamente a gratuidade dos softwares. Hoje, sem sombra de dúvidas, o gratuito é o principal carro chefe da internet, basta pesquisar por essa palavra e uma enxurrada de sites oferecendo produtos de graça surgem na sua tela quase que te obrigando a acessar o produto em questão. No entanto, no mundo o que pouca gente sabe é que a informação mesma é o produto mais valioso da internet.

Segundo Castells (2000, p. 77), não são os bens e serviços que ditam a importância da informação, ao contrário, a informação é um valor em si mesma. Assim, já em 1999 a pesquisadora Darcy DiNucci desenvolveu o conceito *Web 2.0* segundo o qual a web deixaria de ser páginas estáticas e se tornariam ambientes dinâmico e interativos. No entanto, somente em 2004, o conceito se tornou conhecido, quando foi apresentada uma nova forma de desenvolver *software*, não mais em programas desktop, mas em aplicativos web.

O ponto crucial desta inovação seria exatamente a participação dos usuários na manutenção e criação de conteúdo. A partir deste momento, o homem se viu mais inserido na internet e também mais dependente dela, se tornando consumidor e criador de conteúdos e tendências utilizando apenas suas interações com os meios digitais.

Assim, é a internet que estabelece todos os tipos de relações entre as pessoas de todo o mundo, como as sociais, comerciais, judiciais, financeiras e até mesmo as governamentais. À medida que estas relações crescem, igualmente crescem os repositórios de dados contendo todos os dados envolvidos neste vasto número de transações, como documentos, comprovantes, fotos, relatórios, entre outros. São, pois esses dados a alma da *web*.

Com a criação e utilização de tantos dados, é possível levantar e traçar perfis sócio-econômico-culturais que podem ser utilizados para prevenção de evasão fiscal, sugestões de produtos a preços e condições competitivas. Por outro lado, esta tecnologia de processamento de dados pode ser uma grande ameaça à privacidade e à proteção de dados pessoais, como já ficou provado em diversas ocasiões.

É, pois, para garantir a proteção dos dados pessoais, obtidos por meios digitais e respeitado os direitos fundamentais de liberdade e de privacidade, que surgiu a necessidade da formulação de uma lei que proteja os dados pessoais. No Brasil, essa lei foi aprovada via Lei n. 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD).

Inserido neste contexto relativamente novo, este trabalho tem por objetivo analisar e apresentar pontos da LGPD aplicada à área da saúde. Sabe-se que no âmbito da saúde, o prontuário é ferramenta essencial para profissionais da saúde, uma vez que contém todo o histórico de saúde do paciente. Diante disso, o que muda no tratamento do prontuário pela equipe médica?

A Lei geral de proteção de dados: histórico e conceitos

Até a elaboração final da Lei Geral de Proteção de Dados brasileira (LGPD – Lei 13.709/18), um longo caminho foi percorrido ao longo de 8 anos. As discussões começaram em 2010, quando o Ministério da Justiça apresentou à sociedade um anteprojeto para ser debatido através de uma consulta pública. A discussão tinha por objetivo construir um texto democrático para um futuro projeto de lei, esse era um tema considerado como urgente para o governo brasileiro, uma vez que o Brasil era, até então, um dos poucos países da América do Sul que ainda não contava com uma lei específica para proteção de informações pessoais em bancos de dados.

Este artigo foi inspirado na Diretiva 95/46/CE da União Europeia, que disciplinava a proteção de dados, com efeito, a Europa, mais especificamente a Alemanha foi o primeiro país do mundo a se preocupar com a proteção de dados e consequentemente o primeiro também a inserir o conceito de proteção de dados no cenário jurídico, já na década de 1970. Logo em seguida diversos outros países seguiram pelas mesmas vias, como a França, Noruega, Suécia

e Áustria, que criaram suas próprias leis regulamentando informações de seus cidadãos. Logo em 1981, os países membros do então Conselho da Europa desenvolveram e unificaram normas para o tratamento de dados pessoais.

Após as discussões levantadas pela consulta pública de 2010, foram elaborados 3 Projetos de Leis, a PL 4.060/2012, que dispõe sobre o tratamento de dados pessoais, e dá outras providências; a PL 330/2013, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural; e a PL 5.276/2016, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Por fim, em 2018, o Congresso Nacional aprovou o Projeto de Lei nº 53/2018, que fora finalmente sancionado pela Presidência da República em 14 de agosto de 2018. O Brasil finalmente passava a contar com uma Lei Geral de Proteção de Dados, deixando claro logo, no artigo 1º, a sua finalidade.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Destaca-se que a esta lei visa o fomento ao desenvolvimento econômico e tecnológico e também a proteção de direitos e liberdades fundamentais. Para compreender profundamente a LGPD, alguns conceitos são fundamentais, conceitos esses que podem ser relativamente novos no mundo jurídico.

Os dados pessoais dentro do contexto da LGPD têm um papel fundamental, uma vez que é exatamente este o conceito que vai afetar diretamente o escopo da aplicação da lei, aumentando ou restringindo a incidência da norma em diferentes setores.

A definição de tal conceito é apresentado no Art. 5º, inciso I, como sendo toda "informação relacionada a pessoa natural identificada ou identificável". Portanto, trata-se de todo os tipos de informações que permita identificar direta ou indiretamente um indivíduo. A LGPD apresenta um conceito amplo e aberto, deixando a entender que qualquer dado pode ser considerado como dado pessoal.

Sendo assim, dados tais como nome, RG, CPF e endereço, são considerados dados diretos; já dados relacionados à geolocalização de dispositivo móvel, cookies, endereços IP e demais identificadores eletrônicos são considerados dados indiretos.

Na mesma análise de conhecimento dos termos utilizados no contexto da LGPD, encontram-se os dados sensíveis, no mesmo Art. 5º, inciso II apresenta outra categoria de dados pessoais, os dados pessoais sensíveis, que são

> Art 5º II - 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 natural.

Os dados sensíveis ganharam destaque especial, pois o tratamento desses dados exige o consentimento específico e destacado de seus titulares. Há ainda outros dados, que são os chamados dados anonimizados, definido no inciso III do mesmo Art. 5º, como sendo aqueles

dados "relativo a titular que não possa ser identificado". Ou seja, são dados anônimos e que não fazem parte da definição em leis setoriais.

Já o inciso X apresenta o conceito de tratamento de dados, que é:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Pode-se dizer que o fundamento mais importante para se tratar dados pessoais, não é outra coisa senão o consentimento. Sem este instrumento não é possível, ou ilegal qualquer tratamento de dados pessoais. Este é um dos pontos mais delicados para o setor da saúde, como veremos, a seguir.

Apesar de a LGPD ser fortemente baseada no atual Regulamento Geral Europeu, 2016/679, de 27 de abril de 2016, que apresenta regras detalhadas à luz dos avanços tecnológicos, no entanto, a LGPD ainda apresenta alguns problemas conceituais, uma vez que se apresenta muito amplos e sem nenhuma definição clara e específica, o que afeta o escopo de aplicação da lei.

Aspectos gerais do direito à privacidade na área da saúde

A Associação Brasileira de Marketing de Dados (ABEMD) atua diretamente com o desenvolvimento e aprimorando da atuação com o marketing digital no Brasil, sendo referência no processo de esclarecimentos e regulamentações do setor em âmbito nacional, a mesma participou do processo de desenvolvimento da LGPD no Brasil, e entre suas regulamentações é possível encontrar o Código Brasileiro de Auto-regulamentação para a Proteção aos Dados Pessoais, documento que apresenta em seu preâmbulo o objetivo de criar parâmetros para o tratamento de dados pessoais, e entre seus artigos apresenta a responsabilidade pactuada entre as empresas signatárias.

> As empresas e entidades signatárias se comprometem a comunicar ao Conselho Superior de Proteção aos Dados Pessoais de que trata o Capítulo II deste Código, bem como aos titulares dos dados, no prazo máximo de 05 (cinco) dias úteis, sobre o acesso indevido, perda ou difusão acidental, seja total ou parcial, de dados pessoais, sempre que este acesso, perda ou difusão acarretem riscos à privacidade dos seus titulares (ABEMD, 2011).

No setor da saúde, a proteção de dados dos pacientes sempre foi uma dimensão muito séria e por isso mesmo é um tema contemporâneo. No entanto, é insuficiente quando a discussão parte para a privacidade nas práticas em saúde que se utilizam das novas tecnologias de informação e comunicação (TICs), formando assim a sociedade *web* 2.0.

Partindo deste ponto, é importante assumir na mesma sociedade da informação, há também uma sociedade do risco, uma vez que ne sempre o desenvolvimento de novas tecnologias consegue manter a privacidade, gerando consequências graves para a saúde humana. Por outro lado, proteger a privacidade significa garanti-la como direito fundamental baseado e é princípio constitucional, conforme a Constituição brasileira de 1988, que garante, no Capítulo I, Artigo 5º, inciso X, prevê a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Segundo Sarlet (2015, p. 87), garantir a privacidade de informações sobre a saúde das

pessoas significa acima de tudo, neutralizar seu potencial discriminatório. Com efeito, desde 2005, a Organização das Nações Unidas (ONU), chama a atenção para uma "estrutura analítica do direito à saúde", para garantir que a segurança e proteção à vulnerabilidade de certos grupos, como, por exemplos portadores de HIV ou de doenças mentais.

Atualmente, a Organização Mundial da Saúde (OMS) nomeia de e-Saúde (e-*Health*) todos os processos aos quais é utilizada TICs para mediar a atenção à saúde, assistência ao paciente, pesquisa, educação e capacitação da força de trabalho e monitoração e avaliação em saúde. No Brasil, o exemplo mais claro de e-Saúde é o Cartão Nacional de Saúde implantado no Sistema Único de Saúde (SUS).

Através deste sistema, forma-se uma extensão do corpo físico do paciente, formada por dados pessoais que circulam virtualmente, como uma espécie de "avatar" ou "corpo eletrônico". Já na rede privada, a Agência Nacional de Saúde Suplementar (ANS) estabelece medidas padrões obrigatórias na troca de informações entre operadoras de planos de assistência à saúde e prestadores de serviço, garantindo segurança e privacidade.

Apesar do assunto privacidade de dados ser um tema importante na área da saúde, não tem ganhado discussões à altura da importância, como ficou constatado na 14º Conferência Nacional de Saúde de 2012, em temas relacionados à privacidade, sigilo e confidencialidade das informações em saúde, não foram colocados à mesa para discussão, e nem foram contempladas nas diretrizes que visava a exatamente elaborar Política de Informação e Comunicação.

Por outro lado, o Plano Nacional de Saúde, 2016-2019, previa a promoção de ações para assegurar a privacidade e confidencialidade dos aspectos éticos, em todas as etapas do processamento das informações. Já a Política Nacional de Informação e Informática em Saúde (PNIIS) de 2016, ficou estabelecido princípios visando garantir a confidencialidade, o sigilo e a privacidade da informação de saúde pessoal como direito de todo indivíduo.

Diante de toda a fragilidade na garantia à privacidade que a área da saúde no Brasil, a LGPD se mostra como um alento, uma vez que apresenta meios concretos para garantira privacidade, o sigilo e a confidencialidade das informações em saúde. Enquanto isso importantes iniciativas continuam em andamento para desenvolver tecnologias mais seguras, implementar cursos de formação ético-profissional e ampliar a participação social.

Lei geral de proteção de dados aplicada à saúde

O setor da saúde é um dos que mais tratam dados considerados sensíveis e que a sua violação pode acarretar sérios danos ao indivíduo. A LGPD, deixa claro a que tipo de informações o setor da saúde lida (Art. 5º) e de que maneira deve se utilizar dessas informações (Art. 11º). Com efeito, como visto anteriormente o Art. 5º, inciso II define que toda informação que implique "[...] dado referente à saúde ou à vida sexual, dado genético ou biométrico[...]", são considerados dados sensíveis.

Portanto, toda entidade que trata de dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos, é considerada uma empresa cujo dados são sensíveis e por isso mesmo enseja precauções especiais dessa organização. Portanto, qualquer dado pessoal individualizado como, histórico médico, produtos para o cuidado com a saúde, etc, devem ser tratados como dado sensível.

Além dos dados relacionados à saúde, a organizações do setor de saúde ainda lida com uma série de outros dados sensíveis e não sensíveis, como registros financeiros, informações de seguro de saúde, resultados de testes, informações biométricas. Por isso mesmo essas organizações estão em posição crítica na adequação que terá que fazer para se atender as exigências da LGPD.

Outro ponto bastante discutido sobre a aplicação da LGPD é a relação fornecedores terceirizados, que em alguns casos exige a internacionalização do dado pessoal, como por exemplo no uso de tecnologias que envolvem telemedicina. Nessas situações, os dados sensíveis do paciente chegam a outro país e em mãos de outros profissionais.

Uma outra situação que deixa as organizações da área da saúde em complicação é quanto ao uso desses dados sensíveis, uma vez que a lei exige que só pode ser acessado mediante

autorização do titular. Com efeito, o consentimento é o único aval que permita o tratamento dos dados. No entanto, em tratando de saúde, a situação é mais complexa, uma vez que em muitas situações a coleta de dados obtido para uma determinada finalidade, pode posteriormente surgir a necessidade de que esses dados sejam usados para outras aplicações.

Neste caso, a lei determina expressamente que a autorização para uma finalidade diferente daquela originalmente firmada, cabe exclusivamente ao titular, que a qualquer momento tem o direito de voltar atrás em sua decisão de consentimento. Esta nova complicação exige que as organizações criem mecanismos seguros de coleta da autorização do titular e que estejam sempre prontas para produzir, de modo ágil e seguro, provas sobre o aceite em relação ao uso de seus dados.

Por outro lado, essas organizações devem criar instrumentos de monitoramento e controle que permitam a imediata revogação do consentimento, com cessação automática do tratamento dos dados, caso o consentimento não mais seja validado.

A LGPD apresenta algumas hipóteses em que fica autorizada o tratamento de dados sensíveis mesmo sem o consentimento do titular, conforme detalhado no Art. 7º, inciso VIII, "para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária". Este é um caso especial, que na área da saúde pode representar momentos de vida ou morte e para assegurar a vida, a lei permite então que se os dados sensíveis forem indispensáveis ao tratamento, poderão ser utilizados mesmo sem que o seu fornecimento tenha sido consentido pelo titular ou seu responsável.

As organizações que atuam no setor de saúde contam ainda com outras situações previstas na lei para o tratamento de dados sensíveis sem necessariamente precisar da autorização do titular, conforme Art. 7, incisos a seguir:

> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiros;

No entanto, esses casos estão sob a regulação da Agência Nacional de Saúde Suplementar (ANS), cabendo a ela determinar casos específicos de tratamento de dados sensíveis. Desta forma, a ANS pode estabelecer as obrigações que impliquem a delimitação de dados que podem ser tratados e utilizados para apurar doenças pré-existentes, tendências patológicas e outras informações relevantes à mensuração dos riscos envolvidos no seguro do paciente.

Já a hipótese descrita no inciso IV, exige a garantia da anonimização dos dados pessoais sensíveis e isso cabe a qualquer órgão de pesquisa. Esta lei, em específico, exclui a maioria das empresas do mercado de saúde suplementar, que atuam com fins lucrativos ou não possuem finalidade institucional de pesquisa, mesmo quando o objetivo específico daquele tratamento é fundamentalmente desenvolver. Essas empresas ficam possibilitadas de tratar quaisquer dados sensíveis.

Por sua vez, a hipótese prescrita no inciso VII sobre o tratamento de dados sensíveis para proteção da vida ou da incolumidade física não tem nenhuma relação com a hipótese de tutela à saúde prescrita no inciso VIII. O que o inciso VII leva em conta é as situações de riscos à vida ou integridade física relacionados a outras causas, como desastres naturais ou atos de violência. No entanto, como a lei é muito recente, a confirmação dessa interpretação será possível depois de sua aplicação pelas autoridades competentes. Para isso é importante estar atento aos desenvolvimentos da LGPD em casos concretos.

O limite de tratamento de dados aplicado ao setor de saúde é tema fundamental na

LGPD e, de forma especial, para o mercado das operadoras de planos de saúde, uma vez que trata do princípio da não discriminação, definida no Art. 6, inciso IX em que fica impossibilitada o tratamento de dados, diz a lei: "não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Este pode causar impactos importantes aos modelos de negócios das operados de planos de saúde, principalmente no que diz respeito a metodologia de mensuração dos riscos de garantia de cobertura para suas respectivas carteiras de beneficiários. Quais e como calcular as contraprestações que precedem a contratação de planos de saúde sem que se incorra em uma "discriminação abusiva"? Esse assunto com certeza ganhará mais desdobramentos.

Uma possível brecha para as operadoras de planos de saúde seria o compartilhamento de informações de dados. No entanto, a LGPD é bastante taxativa, conforme exposto no § 4º do Art. 11:

> É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde.

No entanto, é possível que haja tal compartilhamento, porém com o consentimento do titular e conformada pelas autoridades competentes. Outro ponto a ser discutido se refere ao trecho "com objetivo de obter vantagem econômica", que pode ser utilizada para se referir a compartilhamentos ou à atividade das empresas controladoras. Com isso, haveria uma disputa em torno do que realmente pretende a lei: vedar o compartilhamento, vedar o compartilhamento para uso com finalidade lucrativa ou, vedar o compartilhamento para uso de empresa que exerça atividade lucrativa? São, pois é outro ponto por não haver clareza levantará bastantes discussões.

Conclusão

Por muito tempo, a saúde é uma das únicas áreas da vida humana em que a privacidade permaneceu altamente sensível. No entanto, à medida que avança os recursos tecnológicos, avança também a falta de privacidade e o que antes era restrito a poucas pessoas, acaba se tornando aberto a uma ampla variedade de profissionais. Um exemplo claro é o caminho para se chegar ao resultado de um único teste. Geralmente são compartilhados com diversos profissionais para se chegar a um diagnóstico. O paciente acaba desconhecendo as informações coletadas, quem tem acesso a elas e como são armazenadas.

A LGPD, pode modificar esse processo, as vezes desconhecido do paciente, ao colocar o indivíduo no comando dos seus dados, desde que a liberdade do paciente em liberar dados para seus médicos de forma remota seja respeitada. Com isso a saúde passará a contar com mecanismos mais transparentes, garantido mais confiança e tranquilidade dos pacientes.

Referências

ABEMD. **Código Brasileiro de Autorregulamentação para a Proteção aos Dados Pessoais**. 2011.

BRASIL, Constituição da República Federativa do. 1998.

BRASIL. **Lei Nº 13.709**, De 14 De Agosto De 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

CASTELLS, Manuel. **The rise of the network society**. 2. ed. The information age: economy, so-

ciety and culture. vol. 1. Massachusetts: Blackwell, 2000.

Sarlet IW, Keinert TMM. O direito fundamental à privacidade e as informações em saúde: alguns desafios. In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB, organizadores. **Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética**. São Paulo: Instituto de Saúde; 2015. p. 113-45.

Recebido em 14 de setembro de 2020.
Aceito em 18 de maio de 2021.