XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

VIVIANE COÊLHO DE SÉLLOS KNOERR

FELIPE CHIARELLO DE SOUZA PINTO

VIRGINIA SUSANA BADO CARDOZO

D597

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Viviane Coêlho de Séllos Knoerr, Felipe Chiarello de Souza Pinto, Virginia Susana Bado Cardozo – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-974-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: ESTADO DE DERECHO, INVESTIGACIÓN JURÍDICA E INNOVACIÓN

1. Direito – Estudo e ensino (Pós-graduação) – 2. Direito e inovação. 3. Propriedade intelectual e concorrência. XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU (2: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA

Apresentação

Texto de Apresentação do Grupo de Trabalho:

DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA I

É com grande satisfação que avaliamos os trabalhos selecionados para o GT DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA I, a coordenação do GT foi composta pelos Professores Doutores Virginia Susana Bado Cardozo da Universidad De La República – UDELAR, Felipe Chiarello de Souza Pinto da Universidade Presbiteriana Mackenzie – MACK/SP e Viviane Coêlho de Séllos Knoerr do Centro Universitário Curitiba – UNICURITIBA, que subscrevemos esta apresentação.

O GT reuniu contribuições significativas que exploram diversos aspectos do atual contexto e abrangência do direito intelectual e concorrencial, refletindo a complexidade e a dinâmica do ambiente jurídico contemporâneo.

Os artigos aqui apresentados oferecem uma análise crítica e inovadora sobre temas variados e atuais. A diversidade dos temas abordados demonstra a amplitude e a profundidade das pesquisas realizadas, tanto no Brasil quanto no Uruguai, contribuindo para o avanço do conhecimento e para a prática jurídica.

Ordem de Publicação dos artigos:

1. A BUSCA PELA PROTEÇÃO DE DADOS SENSÍVEIS EM ÂMBITO HOSPITALAR

2. FAN FICTION: EN BÚSQUEDA DE SU ÁMBITO DE LEGALIDAD

3. INTELIGÊNCIA ARTIFICIAL E ASPECTOS REGULATÓRIOS

4. NOVAS TECNOLOGIAS E O ACESSO À JUSTIÇA

5. O MODELO ONE-STOP SHOP COMO SISTEMA DE GESTÃO DOS DIREITOS AUTORAIS MUSICAIS NO BRASIL

6. PRIVACIDADE E DADOS NA ESFERA DIGITAL

7. REGISTRO CIVIL: DO SURGIMENTO ÀS INOVAÇÕES DAS PRIMEIRAS DÉCADAS DO SÉCULO XXI

8. TECNOLOGIAS DIGITAIS NA ADMINISTRAÇÃO PÚBLICA: TRADE-OFF ENTRE EFICIÊNCIA E ÉTICA

9. VALORAÇÃO DE TECNOLOGIAS: DESAFIOS NO CONTEXTO DO EXÉRCITO BRASILEIRO

As apresentações contextualizaram os artigos e destacaram a importância de cada um dos temas para o avanço do direito e para a cidadania e uma sociedade sustentável, promovendo um debate enriquecedor entre os participantes, verificada a grande participação de pesquisadores de vários estados brasileiros e especialmente, dos nossos anfitriões uruguaios, com o envolvimento notável de professores, pós-graduandos e alunos de graduação, que compartilhando maneiras de enfrentar os problemas levantados, nos presenteiam com textos de recomendada leitura.

Agradecemos ao seleto grupo que conosco integrou o GT DIREITO, INOVAÇÃO, PROPRIEDADE INTELECTUAL E CONCORRÊNCIA I, no CONPEDI internacional 2024, ocorrido na reconhecidamente respeitada e acolhedora UDELAR, em seus 175 anos.

Montevidéu, setembro de 2024.

Os coordenadores

A BUSCA PELA PROTEÇÃO DE DADOS SENSÍVEIS EM ÂMBITO HOSPITALAR

THE SEARCH FOR THE PROTECTION OF SENSITIVE DATA IN A HOSPITAL SETTING

Isadora Moura Fe Cavalcanti Coelho [1]
Juliana Lopes Scariot [2]

Resumo

Diante de frequentes notícias sobre abusos e violações no manejo de informações pessoais e da instabilidade jurídica relacionada ao tratamento de dados, foi promulgada a Lei 13.709/18, mais conhecida como Lei Geral de Proteção de Dados (LGPD). Essa legislação visa estabelecer diretrizes claras para a coleta e o manuseio adequados de dados pessoais, além de impor penalidades para aqueles que os utilizarem de maneira imprópria. Com o rápido progresso tecnológico, a coleta e o armazenamento de dados pessoais têm se tornado mais frequentes e abrangentes, resultando em diversas consequências. Assim, torna-se fundamental que os ambientes que coletam essas informações estejam adequadamente protegidos contra a divulgação não autorizada. Em relação aos dados sensíveis, que serão o tema central do presente estudo, e que cuja exposição pode gerar constrangimento ou preconceito, a necessidade de proteção é ainda mais premente. Por isso, as entidades que lidam com esses dados devem adotar medidas de segurança robustas para evitar a divulgação indesejada, especialmente quando se trata de informações que podem prejudicar a reputação, a integridade ou a dignidade dos indivíduos. Este trabalho, portanto, objetiva informar sobre o direito à privacidade e a Lei Geral de Proteção de Dados, além de destacar a importância da aplicação dessa legislação em hospitais e clínicas de saúde. O método de pesquisa exploratória foi empregado por meio de um levantamento bibliográfico, no qual foram coletadas e analisadas as principais referências relacionadas à temática da Privacidade e da Lei Geral de Proteção de Dados. Esta abordagem foi conduzida de maneira descritiva.

Palavras-chave: Lei geral de proteção de dados, Direito à privacidade, Dados, Vazamento de dados, Lgpd

Abstract/Resumen/Résumé

In light of frequent news about abuses and violations in the handling of personal information and the legal instability related to data processing, Law 13.709/18, better known as the General Data Protection Law (LGPD), was enacted. This legislation aims to establish clear guidelines for the proper collection and handling of personal data, as well as to impose penalties on those who misuse them. With rapid technological progress, the collection and

[1] Mestra em Propriedade Intelectual pela Universidade Federal do Vale do São Francisco. Especialista em Direito Civil em Processual Civil. Advogada. Professora.

[2] Mestranda em Direito Público pela UNISINOS

storage of personal data have become more frequent and extensive, resulting in various consequences. Thus, it becomes essential that environments collecting such information are adequately protected against unauthorized disclosure. Regarding sensitive data, which will be the central theme of this study, and whose exposure can lead to embarrassment or prejudice, the need for protection is even more urgent. Therefore, entities that handle these data must adopt robust security measures to prevent unwanted disclosure, especially when it concerns information that can harm the reputation, integrity, or dignity of individuals. This work aims to inform about the right to privacy and the General Data Protection Law, in addition to highlighting the importance of applying this legislation in hospitals and health clinics. The exploratory research method was employed through a literature survey, in which the main references related to the themes of Privacy and the General Data Protection Law were collected and analyzed. This approach was conducted in a descriptive manner.

Keywords/Palabras-claves/Mots-clés: General data protection law, Right to privacy, Data, Data breach, Lgpd

INTRODUÇÃO

A sociedade moderna enfrenta crescentes preocupações em relação à privacidade. Uma das principais questões é se o conceito de vida privada mantém o significado quando discutido no contexto tecnológico.

No século XVIII, a vida privada era um privilégio reservado a determinadas classes sociais (Prost; Vicent, 2009). E, embora o conceito de privacidade existisse desde essa época, a discussão sobre sua proteção é relativamente recente, especialmente na era digital. Hoje, a privacidade é um dos direitos fundamentais assegurados pela Constituição Federal e tem recebido atenção especial, em parte devido ao comportamento do Estado e de empresas privadas, que têm coletado informações pessoais de maneira irregular e abusiva em busca de vantagens impróprias.

De fato, a coleta de dados é essencial para a eficiência da administração pública e para o crescimento financeiro de empresas privadas. Contudo, a maior capacidade de armazenamento de dados tem facilitado o uso inadequado dessas informações (Toledo, 2020). Por isso, é fundamental proteger o Direito à Privacidade em um mundo cada vez mais orientado pela tecnologia.

Essa questão da privacidade e da segurança dos dados ganhou destaque recorrente na agenda pública devido a vários escândalos de vazamento de dados, tanto nacionais quanto internacionais.

Esses ciberataques frequentemente revelam informações pessoais como CPF, nome, gênero e data de nascimento. Nos últimos anos, o Brasil foi palco de diversos ataques cibernéticos que resultaram na exposição de dados de milhões de pessoas. Um exemplo marcante foi o escândalo de vazamento de dados de 2021, quando aproximadamente 223,74 milhões de registros foram divulgados publicamente em um fórum na internet (Ventura, 2021).

No contexto dos ambientes médico-hospitalares, que constituem o foco principal desta pesquisa, a precaução contra o vazamento de dados deve ser ainda mais rigorosa. Isso se deve ao fato de que esses ambientes lidam com dados sensíveis dos pacientes, cuja divulgação pública pode resultar em constrangimento e preconceito ao indivíduo exposto,

além de prejudicar a reputação e gerar perdas financeiras para a instituição que coleta essas informações.

Os dados sensíveis de saúde incluem detalhes pessoais como diagnósticos médicos, tratamentos e históricos de saúde, que, se divulgados, podem causar danos significativos aos pacientes, comprometendo sua privacidade e dignidade. Além disso, as instituições médicas enfrentam desafios adicionais, pois a exposição desses dados pode minar a confiança dos pacientes, afetando negativamente a reputação da instituição e, em última instância, seus resultados financeiros.

A segurança de dados em ambientes hospitalares é, portanto, fundamental tanto para proteger os pacientes quanto para salvaguardar as instituições. É essencial que essas organizações adotem medidas robustas de segurança cibernética, implementem políticas de privacidade rigorosas e eduquem seus funcionários sobre a importância da proteção de dados. Essas medidas ajudam a minimizar o risco de vazamento de informações e a garantir que as instituições médicas mantenham a confiança do público, além de cumprir com suas obrigações legais e éticas em relação à proteção de dados sensíveis.

Esta discussão é de grande importância, especialmente após a promulgação da Lei 13.709/2018, que trouxe inovações significativas ao ordenamento jurídico brasileiro, estabelecendo novas regras, direitos e princípios para o tratamento de dados pessoais. Além disso, o impacto econômico e regulatório do regime geral de proteção de dados terá reflexos diretos na reputação dos hospitais.

Neste contexto, o presente artigo buscará explorar as diversas facetas da Lei Geral de Proteção de Dados e esclarecer de maneira objetiva como a privacidade se relaciona com o setor da saúde. Para isso, a presente investigação científica está dividida em duas partes: a primeira discorre sobre a Lei Geral de Proteção de Dados (LGPD), regulamentada pela Lei nº 13.709/2018, conceituando o que são dados gerais e dados sensíveis.

Na segunda parte do presente artigo, pois, se discorre acerca da proteção dos dados sensíveis especificamente no âmbito hospitalar, bem como a repercussão de eventual ineficácia desta proteção. Para ambas as partes da investigação, utilizou-se da metodologia científica de revisão narrativa de literatura técnica e jurídica, por meio da técnica exploratória, uma vez que se trata de pesquisa de natureza qualitativa.

1. BREVES COMENTÁRIOS À LEI GERAL DE PROTEÇÃO DE DADOS

Atualmente, é inquestionável a rapidez com que as informações são processadas e disseminadas. Um exemplo marcante desse fenômeno foi observado durante as manifestações populares que ocorreram em 2013, em resposta ao aumento das tarifas de ônibus[1]. Esses protestos rapidamente se espalharam por todo o país, impulsionados pela velocidade do fluxo de informações (Bioni, 2019).

Em seu livro "Proteção de Dados Pessoais: A Função e os Limites do Consentimento", Bruno Ricardo Bioni (2019) discute esse fenômeno, destacando a importância da celeridade na disseminação das informações. Esse contexto evidencia como as tecnologias de comunicação e informação, especialmente as redes sociais e os dispositivos móveis, desempenham um papel fundamental na propagação rápida e ampla de mensagens e eventos.

No entanto, a velocidade do fluxo informacional contemporâneo traz consigo desafios significativos, principalmente no que se refere à veracidade e à confiabilidade das informações compartilhadas. Na era digital, em que a disseminação de conteúdo ocorre em uma escala e velocidade sem precedentes, surgem preocupações substanciais sobre a qualidade e a precisão dos dados que circulam nas redes.

Segundo Bioni (2019), a evolução do uso da informação dentro do contexto da "ciência mercadológica" tem transformado profundamente a maneira como os dados pessoais são valorizados e utilizados. Esta área, que se situa na intersecção do marketing, da tecnologia e da análise de dados, explora como as informações pessoais podem ser empregadas para entender e influenciar o comportamento do consumidor. A partir da coleta e análise de vastas quantidades de dados, as empresas são capazes de criar perfis detalhados dos consumidores, antecipar suas preferências e personalizar produtos e serviços de maneira efetiva.

[1]"Entre 35 mil e 40 mil pessoas, segundo a PM, se reuniram na Esplanada dos Ministérios para protestar contra o preço das passagens de ônibus, os gastos com a Copa das Confederações, a corrupção e as condições da saúde e educação, entre outros temas"(Manifestação em Brasília tem 3 presos e mais de 120 feridos. G1, Disponível em: https://g1.globo.com/distrito-federal/noticia/2013/06/manifestacao-em-brasilia-tem-3-presos-e-mais-de-120-feridos.html. Acesso em 08 maio 2024.

Esse método tem conferido um valor elevado aos dados pessoais, tornando-os uma *commodity* extremamente valiosa no mercado. Por um lado, isso tem possibilitado avanços em personalização e eficiência, permitindo que empresas ofereçam experiências mais alinhadas às expectativas e necessidades dos indivíduos. Por outro lado, levanta questões éticas e legais significativas, relacionadas à privacidade, ao consentimento e à segurança dos dados pessoais.

A preocupação é que, sem regulamentações adequadas e um entendimento claro sobre os direitos e deveres envolvidos na coleta e uso desses dados, pode-se gerar uma exploração abusiva que prejudica a privacidade e a autonomia dos indivíduos.

Portanto, enquanto a ciência mercadológica oferece ferramentas valiosas para o entendimento e a previsão do comportamento do consumidor, ela também exige uma reflexão crítica sobre as implicações éticas e práticas de tais técnicas. Isso inclui debates sobre como assegurar que o uso dos dados pessoais seja conduzido de forma transparente, justa e segura, protegendo os interesses dos consumidores ao mesmo tempo em que se exploram as potencialidades oferecidas pela análise de dados avançada.

Na sociedade moderna, os dados pessoais são cada vez mais valiosos e estratégicos. Eles podem ser empregados em uma variedade de contextos, como na personalização de publicidade e anúncios para consumidores específicos, baseando-se nos sites que visitam na internet (Roque, 2020).

Também podem ser usados para inferir preferências ideológicas ou sexuais por meio da análise de transações feitas com cartão de crédito, ou até para prever doenças que um indivíduo possa vir a desenvolver, através do estudo de seu material genético (Roque, 2020).

Diante da crescente preocupação com a vulnerabilidade das informações pessoais, tanto no ambiente online quanto offline, o Brasil tomou uma medida significativa ao aprovar, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/18). Esta legislação foi promulgada com o objetivo principal de salvaguardar o direito à privacidade e proteger os dados pessoais dos cidadãos brasileiros.

A LGPD estabelece um conjunto abrangente de diretrizes e requisitos que regulam a coleta, o uso, o processamento e a armazenagem de dados pessoais. A lei aplica-se a qualquer operação de tratamento de dados realizada por entidades públicas ou privadas, independentemente do meio, do país de sua sede ou do país onde os dados são localizados, desde que a operação de tratamento seja realizada no território nacional, o

dado seja coletado no território nacional, ou que tenha por objetivo a oferta de bens ou serviços ao território nacional (Brasil, 2018).

A implementação da LGPD foi um passo importantíssimo para alinhar o Brasil às melhores práticas internacionais em privacidade e proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. A lei também criou a Autoridade Nacional de Proteção de Dados (ANPD), um órgão com a função de fiscalizar a aplicação da lei, promover a proteção de dados pessoais e aplicar sanções em caso de violações (Doneda, 2019)

A legislação aborda o tratamento de dados de pessoas naturais, tanto em meios físicos quanto digitais, e estabelece como objetivo a proteção de direitos fundamentais, incluindo liberdade de expressão e comunicação, privacidade, honra, imagem, autodeterminação informativa e o livre desenvolvimento da personalidade (art. 2º). Além disso, a lei salienta que a proteção de dados pessoais serve também para efetivar e promover os Direitos Humanos Fundamentais, constituindo esta uma das justificativas primordiais para a tutela dessas informações (art. 2º, VII) (Mulholland, 2018; Brasil, 2018).

A LGPD foi inspirada na GDPR (General Data Protection Regulation), conhecida nacionalmente como Regulamento Geral de Proteção de Dados da União Europeia, que possui significativa importância global e entrou em vigor em 2016. Esse regulamento europeu também destaca a preocupação com os desafios e consequências decorrentes da coleta e transferência indiscriminadas de dados pessoais (Cavalcanti; Santos, 2018).

> As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global (UNIÃO EUROPEIA, 2016, p.2).

Por isso, a entrada em vigor da Lei Geral de Proteção de Dados, teve um impacto significativo tanto em empresas privadas que manuseiam dados pessoais quanto em órgãos públicos. Isso se deve ao fato de que muitos ainda não se adaptaram completamente às exigências estabelecidas pela legislação, tendo em vista que se trata de uma Lei relativamente recente (com entrada em vigor no ano de 2020).

Essa situação gera uma insegurança jurídica não apenas para as entidades jurídicas que manipulam dados pessoais, mas também para a população em geral, que muitas vezes desconhece como suas informações compartilhadas estão sendo utilizadas (Coelho, 2022).

1.1 Dados gerais e dados sensíveis

A proteção de dados pessoais é uma questão de importância crítica e tem suas raízes na cláusula geral de tutela da pessoa humana, assim como no direito fundamental à privacidade. Essa proteção é um sustentáculo fundamental para a manutenção e o fortalecimento da democracia, garantindo que as liberdades individuais sejam preservadas em um mundo cada vez mais digitalizado e monitorado.

Este direito à proteção de dados pessoais não apenas salvaguarda a privacidade individual, mas também serve como um baluarte contra abusos potenciais por parte de entidades governamentais e corporativas. Na prática, ele permite que os cidadãos mantenham o controle sobre suas próprias informações, decidindo como, quando e por quem esses dados podem ser acessados e utilizados.

Além disso, a proteção de dados fortalece as bases democráticas ao assegurar transparência e responsabilidade no tratamento das informações pessoais. Isso é essencial para a confiança pública nas instituições e nos processos políticos, especialmente em uma era onde as informações podem ser facilmente manipuladas ou exploradas para fins políticos ou econômicos.

Legislações e regulamentações rigorosas, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, exemplificam como os sistemas jurídicos podem se adaptar para proteger os direitos dos indivíduos nesse novo contexto. Esses *frameworks* legais são muito importantes para assegurar que todos os atores – governos, empresas e outras organizações – respeitem os direitos à privacidade e à proteção de dados.

Com o avanço das tecnologias, especialmente aquelas relacionadas à inteligência artificial, a capacidade de tratamento de dados pessoais tem crescido exponencialmente. O desenvolvimento e a aplicação de algoritmos sofisticados, juntamente com técnicas de aprendizado de máquina (machine learning), têm ampliado significativamente as possibilidades de manipulação e análise dessas informações (Mulholland, 2018).

Esse cenário traz tanto oportunidades quanto desafios. Por um lado, a utilização dessas tecnologias pode melhorar a eficiência de serviços e a personalização de experiências, beneficiando tanto consumidores quanto empresas. Por outro lado, o aumento na capacidade de processar e analisar grandes volumes de dados pessoais eleva os riscos de violações de privacidade e de usos indevidos dessas informações.

Em relação ao conceito de dados pessoais, a Diretiva 95/46/CE do Parlamento Europeu estipula que:

> "Dados pessoais" [é] qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, directa (sic) ou indirectamente (sic), nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica (sic), cultural ou social.

Ocorre que, para regular adequadamente as atividades de tratamento de dados, a Lei Geral de Proteção de Dados Brasileira (LGPD) faz uma distinção entre dois tipos de informações: dados pessoais e dados pessoais sensíveis.

Conforme definido no artigo 5º, I da LGPD, um dado pessoal inclui qualquer informação que possa identificar uma pessoa natural, ou torná-la identificável. Isso abrange uma gama ampla de informações, desde o nome e o número do CPF até detalhes como endereço de e-mail ou localização geográfica (Brasil, 2018).

Por outro lado, os dados pessoais sensíveis, descritos no artigo 5º, II da lei, concernem a aspectos mais delicados da esfera pessoal, que exigem uma proteção ainda mais rigorosa devido ao potencial de discriminação ou abuso. Esses dados incluem informações sobre a origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical ou a organizações de natureza religiosa, filosófica ou política, além de dados relacionados à saúde, à vida sexual, e informações genéticas ou biométricas que estejam vinculadas a uma pessoa natural (Brasil, 2018).

Sobre isso:

> O regime adotado em relação aos dados sensíveis varia de acordo com as concepções a este respeito em cada ordenamento jurídico. Em verdade, é necessário ter em conta que a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações nas quais a discriminação pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos. (Doneda, 2019, P. 144).

Complementando:

> […] coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como "a proteção de escolhas de vida contra qualquer forma de controle público e estigma social" (L. M. Friedman), como a "reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto" (J. Rosen). (Rodotà, 2008 p. 12)

A diferenciação entre esses dois tipos de dados na LGPD visa não apenas proteger a privacidade dos indivíduos, mas também prevenir o uso discriminatório ou prejudicial dessas informações. Isso implica que qualquer entidade que lide com dados sensíveis deve seguir protocolos de segurança mais estritos e garantir que o consentimento para seu tratamento seja explícito e inequívoco, assegurando a proteção efetiva dos direitos fundamentais das pessoas naturais.

Importante mencionar que a Lei Geral de Proteção de Dados confere uma proteção excepcional aos dados sensíveis, dado que eles tocam nos aspectos mais íntimos da privacidade humana e podem levar a consequências discriminatórias.

No contexto da saúde, o tratamento desses dados é particularmente delicado. Isso ocorre porque os dados de saúde são considerados sensíveis e, portanto, exigem uma vigilância e cuidado redobrados por parte dos responsáveis pelo seu tratamento. Além disso, é impossível realizar um atendimento médico adequado sem o compartilhamento de informações cruciais como histórico de saúde, uso de medicamentos, diagnósticos e resultados de exames, que compõem o prontuário médico.

2. DA NECESSIDADE DA OBSERVÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS EM ÂMBITO HOSPITALAR

Como já destacado, os dados pessoais são ativos valiosos e intangíveis para os indivíduos. Os dados sensíveis, em particular, possuem ainda maior valor, dado que, conforme estabelecido pela Lei 13.709/18, são informações cuja revelação indevida pode causar constrangimento e discriminação significativa tanto para o indivíduo quanto para sua família, especialmente em casos de vazamentos (Coelho, 2022).

Os dados sensíveis relacionados à saúde estão entre os mais valiosos no mercado de informações, uma realidade amplamente reconhecida devido à longevidade desses registros nas bases de dados das instituições médico-hospitalares (Trustwave, 2022).

> O acesso descontrolado e o uso indevido dos dados de saúde, igualmente denominados dados clínicos ou informações médicas, banalizam o direito à privacidade do indivíduo, que não raramente desconhece o destino de seus registros. A autodeterminação informativa do paciente é fundamento da LGPD, conforme preconiza o art. 2º, II, e inicia-se a partir do preenchimento do termo de consentimento esclarecido e informado, documento exigido para procedimentos ou intervenções cirúrgicas, bem como para a realização de pesquisas.
>
> Tais atos necessitam de dados de saúde e os termos de consentimento que eles exigem devem conter avisos relativos ao grau de confiabilidade de exames, alertas de possíveis riscos, consequências fisiológicas e complicações, além do caráter, objetivos e benefícios da intervenção (Zaganelli; Filho, 2022).

O setor de saúde é particularmente vulnerável a violações de dados, uma realidade exacerbada pela alta sensibilidade das informações que maneja. Invasores utilizam técnicas avançadas como data mining para extrair dados confidenciais e torná-los públicos (Abouelmehdi; Beni-Hessane e Khaloufi, 2018).

Um exemplo notório dessa vulnerabilidade ocorreu em novembro de 2020, quando uma falha de segurança no sistema do Ministério da Saúde do Brasil resultou na exposição de dados de 16 milhões de pessoas com diagnóstico suspeito ou confirmado de Covid-19. Apenas um mês depois, outra falha de segurança expôs dados pessoais de mais de 200 milhões de brasileiros, incluindo usuários do Sistema Único de Saúde e de planos de saúde privados, como reportado por Bertoni (2020).

> De acordo com dados colhidos no HIPAA Journal, entre 2009 e 2020, 3.705 violações de dados de saúde de 500 ou mais registros foram relatadas ao Gabinete de Direitos Civis de Saúde e Serviços Humanos dos Estados Unidos da América.
>
> Essas violações resultaram na perda, roubo, exposição ou divulgação inadmissível de 268.189.693 registros de saúde. Isso equivale a mais de 81,72% da população dos Estados Unidos. Em 2018, violações de dados de saúde de 500 ou mais registros estavam sendo relatadas a uma taxa de cerca de 1 por dia. Em dezembro de 2020, essa taxa dobrou. O número médio de violações por dia em 2020 foi de 1,76 (Zaganelli; Filho, 2022).

Essa vulnerabilidade decorre tanto do valor intrínseco dessas informações quanto da natureza permanente de seu armazenamento. Dados de saúde contêm detalhes íntimos sobre a condição física e mental dos pacientes, informações essas que, se expostas ou manipuladas erroneamente, podem resultar em sérias consequências pessoais e financeiras (Korkmaz e Negri, 2019).

Por isso, é fundamental que as instituições de saúde implementem medidas de segurança rigorosas e mantenham uma vigilância constante sobre suas bases de dados para prevenir abusos e garantir a proteção da privacidade dos pacientes.

Na contemporaneidade, a área da saúde tem testemunhado uma rápida transformação impulsionada pelo avanço tecnológico. A adoção crescente de recursos como a telemedicina, sistemas de prontuários eletrônicos e o armazenamento de dados digitais essenciais para o cuidado do paciente tem revolucionado a maneira como os profissionais de saúde interagem com as informações clínicas (Martins; Teles, 2021).

Anteriormente, com os métodos manuais de registro e compartilhamento de dados, o intercâmbio de informações na área da saúde era limitado e muitas vezes demorado. Os registros eram armazenados em papel, tornando a recuperação e o compartilhamento de informações um processo trabalhoso e suscetível a erros. Além disso, a comunicação entre diferentes profissionais de saúde e instituições muitas vezes era difícil, o que poderia comprometer a continuidade do cuidado do paciente (Coelho, 2022).

Com o advento da tecnologia, especialmente dos sistemas de informação em saúde, houve uma revolução nesse cenário. A implementação de sistemas de prontuários eletrônicos permite o armazenamento seguro e acessível de informações médicas, facilitando o compartilhamento rápido e eficiente entre profissionais de saúde e instituições de saúde.

Isso significa que médicos, enfermeiros e outros membros da equipe podem acessar facilmente o histórico médico completo de um paciente, incluindo resultados de exames, prescrições médicas e notas de procedimentos anteriores.

> Considerando as consultas médicas realizadas por meio da técnica da telemedicina, fica claro que, o médico, utilizará o sistema de informática como ferramenta de trabalho, tendo à sua disposição, ferramentas úteis para o tratamento e formatação dos dados fornecidos por seus pacientes. A hipótese que se coloca é no sentido de qual a natureza da responsabilidade civil do médico quando realiza o tratamento de dados do paciente violando os direitos fundamentais de liberdade, de privacidade e/ou do livre desenvolvimento da personalidade da pessoa natural (Martins; Teles, 2021).

No entanto, esse aumento na troca de informações também traz desafios, especialmente no que diz respeito à segurança e privacidade dos dados do paciente. É essencial garantir que as informações de saúde sejam protegidas contra acessos não autorizados e que sejam adotadas medidas rigorosas para proteger a confidencialidade dos dados dos pacientes.

De acordo com um estudo realizado pelo *Trustwave Global Security Report* em 2019, um registro médico pode alcançar até duzentos e cinquenta dólares no mercado ilegal da “dark web”. A pesquisa destacou que as informações relacionadas à saúde dos pacientes são consideradas muito mais valiosas do que os dados de cartões de crédito. Isso se deve ao caráter extremamente pessoal e sensível dessas informações.

Neste contexto, empresas desonestas podem explorar esses dados de saúde de maneira imprópria para promover seus interesses comerciais. Da mesma forma, criminosos podem se aproveitar desses dados para cometer atos de extorsão, utilizando informações sensíveis para coagir indivíduos. Além disso, em cenários políticos, um candidato antiético poderia usar informações sobre a saúde de um oponente para comprometer sua imagem e reduzir suas chances em uma eleição (Klajner, 2022).

Portanto, a integridade e a segurança dos dados de saúde são de extrema importância, exigindo medidas rigorosas de proteção para prevenir o uso indevido e as consequências danosas que podem advir de tal exposição.

> É preciso que fique nítida a necessidade de uma segurança quanto ao tratamento de dados na saúde, pois a coleta de dados dos pacientes é diária, e, quando uma instituição se encontra respaldada perante a lei de proteção de dados, ela transmite uma confiança e segurança para seus

> pacientes, informando como esses dados serão armazenados, para qual fim, deixando-os em uma situação confortável de escolha quanto as informações passadas. (LGPD BRASIL, 2022).

Ou seja, é necessário que se abram os olhos para a importância crítica de implementar medidas rigorosas de segurança no tratamento de dados na área da saúde. A coleta diária de dados dos pacientes só evidencia a necessidade de as instituições estarem plenamente em conformidade com a legislação de proteção de dados.

Quando uma instituição de saúde demonstra estar alinhada com esses requisitos legais, ela não apenas cumpre com as normativas, mas também transmite uma sensação de confiança e segurança aos seus pacientes.

Ao informar claramente como os dados são armazenados, os propósitos de seu uso e garantindo a transparência, as instituições colocam os pacientes em uma posição confortável para fazer escolhas informadas sobre as informações que compartilham. Isso não só fortalece a relação entre pacientes e provedores de serviços de saúde, mas também assegura a proteção de informações sensíveis, reforçando o compromisso com a ética e a responsabilidade no manejo dos dados pessoais.

CONCLUSÃO

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) em 2018 representou um divisor de águas para as empresas brasileiras, sobretudo para o setor de saúde, que teve que acelerar processos de conformidade para atender às rigorosas demandas impostas pela legislação.

A principal exigência da LGPD é a garantia de segurança para os titulares dos dados, uma necessidade que impulsiona clínicas e hospitais a implementar sistemas de segurança avançados e confiáveis.

Dentro desse contexto, as instituições de saúde enfrentam o desafio de proteger dados altamente sensíveis, como informações médicas pessoais, que exigem não apenas o cumprimento das normas legais, mas também a adoção de práticas que assegurem a integridade e a confidencialidade dessas informações. Isso envolve desde a implementação de tecnologias de criptografia e segurança cibernética até o treinamento contínuo de pessoal para lidar com esses dados de maneira responsável.

Além disso, a adequação à LGPD e a adaptação às novas tecnologias devem andar lado a lado, garantindo que os direitos à privacidade e à proteção da pessoa humana sejam efetivamente preservados na era digital.

Anteriormente, quando as instituições dependiam de documentos físicos, a segurança consistia principalmente em manter os locais de armazenamento trancados. Os hospitais são obrigados a conservar prontuários físicos por pelo menos vinte anos para determinadas condições médicas, e esse período pode ser estendido dependendo de outras circunstâncias.

É certo que, com a digitalização desses documentos, a gestão e o armazenamento tornaram-se mais eficientes, mas isso também aumentou a necessidade de garantir a disponibilidade e a segurança dessas informações digitalizadas. As instituições de saúde normalmente desenvolvem suas próprias políticas de segurança da informação, incluindo processos especializados para detecção e classificação de riscos.

Isso significa que as políticas de governança de dados precisam ser dinâmicas e se adaptar continuamente às novas realidades tecnológicas e aos desafios emergentes, assegurando um tratamento ético e transparente dos dados pessoais.

Essa evolução constante é fundamental para manter a confiança do público e para que as instituições de saúde possam não apenas cumprir com suas obrigações legais, mas também promover um ambiente de segurança e confiança que seja fundamental para a relação entre pacientes e provedores de serviços de saúde.

REFERÊNCIAS

Abouelmehdi, K., Beni-Hessane, A.; Khaloufi, H. (2018) **"Big healthcare data: preserving security and privacy".** Journal of Big Data, El Jadida, 5, 1, 1-18. Disponível em: https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-017-0110-7.pdf. Acesso em: 08 mai. 2024.

Bertoni, E. (2020) **"O novo vazamento de dados na Saúde. E suas consequências".** Nexo, 2 dez. 2020. Disponível em: https://www.nexojornal.com.br/expresso/2020/12/02/O-novovazamento-de-dados-na-Saúde.-E-suas-consequências. Acesso em: 09 mai. 2041.

BIONI, Bruno Ricardo, **Proteção de dados pessoais: a função e os limites do conhecimento**, Rio de Janeiro: editora Forense, 2019., p 34.

BIONI, Bruno Ricardo. **Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. [S.l.: s.n.], 2016. Disponível em:<https://www.researchgate.net/publication/328266374_XequeMate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil>. Acesso em: 04 Mai. 2024.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União (DOU), Brasília, DF, 15 ago. 2018.

CAVALCANTI, N; SANTOS, L. **Lei Geral de Proteção de Dados do Brasil na Era do Big Data**. In: FERNANDES, R; CARVALHO, A. Tecnologia Jurídica & Direito Digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018, Belo Horizonte: Fórum, 2018. p. 351 -365.

COELHO, Isadora Moura Fé Cavalcanti. **A Implementação de Políticas de Privacidade e a Lei Geral de Proteção de Dados: A Necessidade de Preservação de Dados Sensíveis no Âmbito da Saúde.** Dissertação de mestrado para o Programa de Pós Graduação em Propriedade Intelectual e Transferência de Tecnologia para Inovação, Universidade Federal do Vale do São Francisco. Juazeiro, 2022.

DONEDA, Danilo**. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

KLAJNER, Sidney**. LGPD: Quem é responsável pela proteção dos seus dados de saúde?** 2022, disponível em < https://www.jota.info/opiniao-e-analise/artigos/lgpd-quem-e-responsavel-pela-protecao-dos-seus-dados-de-saude-30052022> Acesso em 09 mai. 2024.

LGPD BRASIL, **Adequação da LGPD na saúde: entenda mais**. LGPD Brasil, 2022. Dísponível em <https://www.lgpdbrasil.com.br/lgpd-na-saude/> Acesso em 09 mai 2024.

Martins, G. M., & Teles, C. A. C. A TELEMEDICINA NA SAÚDE SUPLEMENTAR E A RESPONSABILIDADE CIVIL DO MÉDICO NO TRATAMENTO DE DADOS À LUZ DA LGPD. ***REI - REVISTA ESTUDOS INSTITUCIONAIS*****,** 2021.

MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais: Uma Análise à Luz da Lei Geral de Proteção de Dados**. R. Dir. Gar. Fund.,** Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018

PROST, Antoine; VINCENT, Gérard (Org.). **História da vida privada**. 1. Ed. Tradução de Denise Bottmann, Dorothée de Bruchard. São Paulo: Companhia das Letras, 2009. v. 5.

ROQUE, André. A Tutela Coletiva dos Dados Pessoais na Lei Geral de Proteção de Dados Pessoais. **Revista Eletrônica de Direito Processual –REDP**. Rio de Janeiro. Ano 13. Volume 20, 2020.

TOLEDO, Mariana. **Imersão LGPD**. Primeira Live. Elaborado por @creation.space_. Copyright 2020.

TRUSTWAVE, Resource Library, **Global Security Report**, 2019, disponível em <https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report-executive-summary/>. Acesso em 06/05/2024

UNIÃO EUROPEIA. **Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 4 maio 2016. Disponível em: Acesso em: 4 mai 2024

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados**). Jornal Oficial da União Europeia, Estrasburgo, 24 out. 1995. Disponível em: Acesso em: 4 mi 2024.

Ventura, F. (2021**) "Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava"**. Tecnoblog, 22 jan. de 2021. Disponível em: https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-debrasileiros-e-pior-do-que-se-pensava/. Acesso em: 20 fev. 2021.

ZAGANELLI, Margareth Vetis; FILHO, Douglas Luis Binda; A Lei Geral de Proteção de Dados e suas implicações na saúde: as Avaliações de Impacto no tratamento de dados no âmbito clínico-hospitalar. **Revista de Bioética y Derecho Perspectivas Bioéticas. 2022.** Disponível em: https://scielo.isciii.es/pdf/bioetica/n54/1886-5887-bioetica-54-215.pdf. Acesso em 09 mai. 2024.