

O DIREITO À PROTEÇÃO DE DADOS DOS USUÁRIOS DE SERVIÇOS DE SAÚDE EM HOSPITAIS

The Right To Data Protection Of Users Of Health Services In Hospitals

Cláudio José Franzolin

Pontifícia Universidade Católica de Campinas

Andressa Sanchez Silva Luizon

Pontifícia Universidade Católica de Campinas

RESUMO

O presente artigo intenciona a análise da proteção de dados no contexto do direito à privacidade de pacientes, notadamente os usuários de hospitais. Para tanto, o primeiro capítulo aborda a necessidade de limitação dos serviços tecnológicos em detrimento à proteção da intimidade e privacidade, como forma de preservar a dignidade da pessoa humana. Por sua vez, no segundo capítulo busca-se a intersecção entre o direito e a medicina a fim de compreender a despeito do dever de sigilo médico como um reflexo do direito da confidencialidade das informações do paciente. Por fim, o terceiro capítulo abarca a necessidade urgente de adaptação para além da implementação de novas tecnológica, mas, sobretudo, de treinamento de funcionários, para proteger informações médicas referente ao quadro clínico e, dados pessoais, dos pacientes que foram atendidos naquele sistema de saúde.

Palavras-chave: Proteção de dados de saúde; Direito Médico; Confidencialidade.

ABSTRACT

This article intends to analyze data protection in the context of the right to privacy of patients, notably hospital users. To this end, the first chapter addresses the need to limit technological services to the detriment of the protection of intimacy and privacy, as a way of preserving the dignity of the human person. In turn, the second chapter seeks the intersection between law and medicine in order to understand despite the duty of medical secrecy as a reflection of the right to confidentiality of patient information. Finally, the third chapter covers the urgent need for adaptation beyond the implementation of new technologies, but, above all, employee training, to protect medical information regarding the clinical condition and personal data of the patients who were treated in that system. health.

Keywords: Health data protection; Medical Law; Confidentiality.

INTRODUÇÃO

Com o avanço tecnológico cada vez mais presente na sociedade contemporânea, torna-se de suma importância atentar-se ao direito à privacidade, inclusive por ser direito fundamental que deve ser tutelado.

O direito fundamental à privacidade encontra fundamento axiológico na dignidade da pessoa humana, projetando-se como dimensão estruturante da identidade social do indivíduo (Paiano, 2003), o que impõe ao ordenamento jurídico o dever de assegurar sua proteção efetiva, tanto na esfera negativa (de não ingerência) quanto na dimensão positiva de garantia, assegurando ao titular a fruição plena de sua autodeterminação e o controle sobre as informações que o dizem respeito.

Desta feita, o objetivo deste trabalho é analisar o impacto advindo dos serviços ofertados por hospitais, notadamente relacionados à saúde e gestão hospitalar administrativa, frente à informação de saúde dos pacientes.

Para tanto, utilizou-se o método hipotético dedutivo de cunho empírico, cujo argumento principal se pautou na tendência de captação de dados com utilização de inteligência artificial e algoritmos, nas condutas médicas hospitalares, tendo como documento autorizador tão somente o termo de consentimento pré formulado assinado pelo paciente e de acesso aberto por terceiros além do médico que tenha realizado o atendimento.

Em complemento, esta pesquisa também considera como referencial de estudo a Lei de Proteção de Dados, promulgada sob a numeração 13.709, de 14 de agosto de 2018, e demais diplomas nacionais e internacionais a respeito.

Atenta-se para o fato de que estamos inseridos em uma sociedade marcada por práticas difusas e permanentes de vigilância, na qual a concepção clássica de privacidade como “right to be let alone” (Brandeis; Warren, 1890) mostra-se insuficiente diante da complexidade da sociedade informacional descrita por Castells (2019), emergindo o direito à autodeterminação informativa como paradigma normativo adequado. Nesse contexto, a dimensão física e digital do sujeito, *i.e.*, sua corporeidade e sua projeção eletrônica, bem como sua identidade individual e social, passam a depender diretamente da proteção de dados pessoais, da preservação da liberdade individual e das condições de coexistência social, fortalecendo o vínculo entre dignidade e tutela informacional (Moraes, 2010).

A identidade social, enquanto elemento constitutivo da personalidade, adquire centralidade por possibilitar ao indivíduo estar e ser no meio social mediante o reconhecimento de sua autonomia nas tomadas de decisões, direito ao sigilo e ao controle informacional, atributos que encontram fundamento normativo na dignidade humana como valor-fonte do sistema constitucional, eixo da efetividade de direitos fundamentais relacionados à personalidade.

Nesse cenário, ao considerarmos a sociedade pós-moderna de Lipovetsky (2004), a liberdade de escolha deixa de ser um conceito abstrato e passa a exigir uma retração da ingerência estatal. Essa autonomia privada, contudo, só se sustenta se acompanhada de novos mecanismos de salvaguarda da privacidade, como destaca Luizon (2025): “a autodeterminação, pois, refere-se ao direito de receber informação e decidir sobre os atos de sua vida [...]”.

A expansão das escolhas individuais conecta-se diretamente à noção jurídica de autodeterminação existencial; dimensão do princípio da liberdade (Da Silva, 2021); no entanto, a realidade tem mostrado que as tecnologias disruptivas têm contribuído para direcionar os cidadãos para esta ou aquela condução. Tema este que deve ser debatido noutra oportunidade e não este estudo. De qualquer modo, surgem traduzidas em decisões existenciais acompanhadas de juízos axiológicos próprios, que devem ser exercidas sem ingerências arbitrárias ou restrições desproporcionais impostas pelo Estado.

Todavia, conforme leciona Sarlet (2018), tal concepção não exclui a legitimidade da intervenção estatal quando indispensável à salvaguarda da privacidade. Incumbe ao Estado não apenas o dever de abstenção, mas também o dever de proteção (*Schutzpflicht*). Isso exige a adoção de medidas normativas e institucionais que assegurem o livre desenvolvimento da personalidade, garantindo ao paciente condições de igualdade material e dignidade frente a possíveis abusos de terceiros.”

Desse modo, o livre desenvolvimento da personalidade impõe a superação da concepção reducionista do “direito de ser deixado só”, afirmando-se como direito à autodeterminação informativa; o enfoque é promover a titularidade do cidadão sobre seus dados pessoais para que ele gerencie, permitindo ao titular exercer controle qualificado sobre seus dados pessoais, definindo as finalidades de seu tratamento e estabelecendo os contornos de sua própria esfera privada informacional, afinal, a autodeterminação informativa está relacionada com a proteção de dados, a qual deve ser reconhecida como direito fundamental autônomo, integrante do núcleo essencial dos direitos da personalidade no cenário digital (Doneda, 2002).

É neste contexto a presente pesquisa se desenvolve tendo como escopo a importância da privacidade e da proteção de dados dos usuários de serviços de saúde, contribuindo na expansão das discussões sobre o atual cenário em que a inteligência artificial vem sendo integralizada no atendimento médico hospitalar.

A proteção de dados e o Direito Médico

No que tange à Deontologia Médica, o sigilo profissional e, como corolário lógico, a confidencialidade das informações prestadas pelo paciente, remontam desde Hipócrates, transformando-se em uma obrigação legal e ética (Robl Filho, 2006).

Em um breve esboço histórico concernente à Deontologia Médica, percebe-se a importância e revisão da temática da privacidade, como se observa, por exemplo, na Declaração de Genebra em 1948 (reforçando o

compromisso médico com a privacidade); Declaração de Helsinque em 1964 (reforçando princípios éticos); American Hospital Association Patient's Bill of Rights de 1973, acerca dos princípios e direitos fundamentais dos pacientes, cujo quinto direito contempla a privacidade, principalmente para realização de tratamentos e consultas, exames médicos etc.; Genetic Privacy Act, de 1995, com objetivo de proteger a privacidade genética; Declaração Universal sobre o Genoma Humano e Direitos Humanos, de 1997; Declaração Internacional da UNESCO sobre os Dados Genéticos Humanos, de 2003; Declaração Universal sobre Bioética e Direitos Humanos, de 2005 (acerca da privacidade e confidencialidade das informações dos pacientes, enaltecendo o princípio da finalidade).

Emerge-se que qualquer afronta à intimidade ou à vida privada do paciente configura violação direta à dignidade da pessoa humana e aos fundamentos da cidadania previstos no art. 1º, III, da Constituição Federal, ensejando responsabilização nas esferas civil, administrativa e, quando cabível, penal, além de integrar o dever institucional de proteção de dados e de observância das normas de governança hospitalar.

E dentro dessa perspectiva de proteção de dados e informações do paciente, deve-se observar a forma de gestão e administração desses em sistemas computadorizados de hospitais.

Isso porque a violação de direitos do paciente, inclusive no que tange ao acesso indiscriminado de informações e dados, geram deveres legais, culminando, pois, a partir da entrada em vigor da LGPD, na obrigação de adotar medidas que mitiguem os riscos daí decorrentes e procedimentos de controle e armazenamento seguros de dados, para que não ocorra situações de disponibilização para terceiros sem o devido consentimento.

Importa destacar que a intimidade é a esfera de pertencimento exclusivo, cuja lesão pode materializar-se tanto pela obtenção indevida de informações, mediante práticas ilícitas, abusivas ou desproporcionais, quanto por sua divulgação não autorizada, considerando que o direito à intimidade visa resguardar o indivíduo contra ingerências externas capazes de comprometer sua esfera existencial (Ferraz Junior, 2003).

Por sua vez, a confidencialidade é uma *fatie specie* do gênero privacidade (Faria; Cordeiro, 2014), sendo que, na área de saúde tem o condão de vedar e limitar a divulgação de informações relativas ao paciente (Beauchamp; Childress, 2009), abrangendo uma gama de direitos que transcende a mera proteção de dados, englobando todas as informações; tais como comportamentos de riscos, hábitos de vida, exames, e etc., que devem estar fora do domínio público e que se relaciona com a fidúcia do paciente depositada no profissional da saúde.

A fidúcia do paciente, i.e., a confiança depositada no médico que atende no hospital, e, portanto, também na pessoa jurídica "hospital", advém do resultado da certeza e previsibilidade, do paciente, de que todas as informações que lhe dizem respeito serão respeitadas e abordadas com segurança sem repercussões negativas em sua vida, mas tão somente para o seu tratamento (Villas-Bôas, 2015).

O consentimento, por sua vez, se materializa de forma explícita a partir da assinatura dos pacientes ao documento respectivo, mas, para que esse documento tenha validade jurídica questiona-se se no momento da assinatura do termo de consentimento o paciente, de fato, deveria ter recebido explicações, em linguagem acessível, de modo a garantir o entendimento quanto ao tratamento de seus dados coletados, ou, apenas o aceite documentado pela assinatura seria o suficiente para demonstrar o respeito ao cumprimento legal do inciso XII, do artigo 5^a da LGPD.

Outro ponto importante a ser observado nessa relação médico-paciente é a possível flexibilização do sigilo médico quando se trata de dados e informações inseridas em sistema computadorizado do hospital, pois embora o meio eletrônico possa majorar o risco de interceptação por terceiros, ao mesmo tempo é forma evitar erros técnicos de procedimento e possível integração com outros profissionais da saúde.

Nesse ínterim, importante frisar que o sigilo das informações e dados dos pacientes não abrange tão somente os médicos, mas também todos aqueles que, direta ou indiretamente, em sua atividade diária hospitalar, podem ter acesso à estas informações (secretaria, enfermagem, outros pacientes, setores da administração, setor de limpeza etc.), uma vez que a ética profissional imprime aos responsáveis direta ou indiretamente a responsabilidade da confidencialidade, somado ao teor da Lei de Proteção de Dados e do artigo 154 do Código Penal.

Diante da manutenção de controle, pelo hospital, dos dados do paciente e da sua confidencialidade, é necessário garantir proteção a estes dados para que eventual disponibilização, comercialização ou utilização ilegal - inclusive após o óbito do paciente, não ocorra, pois a LGPD veda o compartilhamento e a comunicação do controlador dos dados pessoais e sensíveis concernentes à saúde, com o objetivo de obtenção econômica, sendo que a devassa dos dados de saúde e médicos são considerados ainda mais grave por estarem sob o mantra dos dados sensíveis (Brasil, 2023).

A proteção de dados do paciente

Não se pode desconsiderar a complexidade estrutural e operacional inerente à implementação da LGPD no contexto brasileiro, especialmente em instituições hospitalares de grande porte, nas quais o fluxo massivo de dados sensíveis impõe elevados padrões de governança informacional, acarretando fragilidade no manejo dos dados pessoais e sensíveis dos pacientes, *i.e.*, troca e venda destas informações (o que pode ocorrer), e, a partir daí, acarretar discriminações, à exemplo, de inserção no mercado de trabalho ou modulação de preços em serviços ofertados pelas seguradoras de saúde ou vendas de medicamento, circunstância que evidencia a necessidade de harmonização normativa e cooperação regulatória, inclusive em âmbito transnacional, diante da circulação global de dados e da interconectividade dos sistemas digitais (Stelzer, 2009).

Apesar dos desafios que a implementação da LGPD está enfrentando no que tange à sua efetividade na proteção dos dados e informações na rede virtual, como, por exemplo, a mudança de identificação ou mesmo a

retirada da anonimidade dos dados de indivíduos em sistemas que utilizaram técnicas de encriptação de dados (OHM, 2010), algumas medidas podem contribuir para a efetividade da proteção da confidencialidade; treinamento básico sobre T.I. (Tecnologia de Informação) aos profissionais de saúde em relação à proteção de dados, diminuindo a necessidade de recursos externos e terceirizados; criação de avaliação de impacto periódico com o objetivo de identificar riscos e falhas, no intuito de reavaliação de protocolos e procedimentos protetivos.

Estas medidas, exemplificativamente acima elencadas, colaboram para que não haja violação da confidencialidade dos dados do paciente, evitando acessos indevidos nos registros e vedando a participação de pessoas que não se encontram envolvidas diretamente nos serviços médicos e de saúdes ofertados pelo hospital, havendo como consequência também, a maior conscientização dos profissionais envolvidos acerca do sigilo profissional e da confidencialidade daí decorrente.

Entretanto, para que as medidas protetivas tenham eficácia em âmbito hospitalar é necessário, primeiramente, que haja ampla compreensão pelos envolvidos acerca da forma como os dados e informações dos pacientes são coletadas pelo hospital, tanto de forma digital quanto em registros documentais físicos.

O volume de dados sensíveis associados à saúde do paciente pode ser suscetível de riscos, tais quais, extravio de informações; perda da confidencialidade de determinado dado por falha de acesso; utilização dos dados para fins investigativos, científicos ou acadêmicos sem o conhecimento dos pacientes; transferência, comercialização ou envio ilícito dos ditos dados.

Ademais, em relação aos dados pessoais, é necessário respeitar diversos princípios (Doneda, 2011), tais como o princípio da correção (garantia ao paciente de adequar e corrigir seus dados); princípio da exatidão das informações; princípio da finalidade (dados pessoais do paciente devem obedecer uma finalidade previamente comunicada pelo profissional da saúde, principalmente antes da coleta); princípio da publicidade; princípio da segurança no local da coleta de dados (os dados pessoais coletados pelo hospital devem ser protegidos em face de acesso não autorizado de terceiros, extravio, destruição, modificação etc.); princípio da temporalidade (os dados coletados pelo hospital não devem permanecer sob sua posse por tempo indeterminado, principalmente após o óbito do paciente); princípio da relevância e da proporcionalidade (a coleta de dados pessoais pelo hospital deve ser a mínima possível e, havendo alternativa menos gravosa, esta que deverá ser adotada).

Para que haja o respeito aos princípios norteadores da coleta e armazenamento de dados pelo hospital é imprescindível que haja uma fiscalização rígida de como os hospitais armazenam os dados pessoais e sensíveis dos pacientes, principalmente àqueles relacionados à saúde, mapeando e identificando atos discriminatórios e coletando dados para fins estatísticos acerca da empregabilidade dos dados dos pacientes nestas circunstâncias.

Outrossim, a partir da leitura acurada da LGPD, especificamente no inciso XII, do artigo 5º, percebe-se que somente o termo de consentimento assinado pelo paciente não é o suficiente para dirimir a questão da coleta e do armazenamento indiscriminado de dados, isso porque exige-se que o paciente tenha recebido prévio e inequívoco esclarecimento a respeito do tratamento de seus dados, com destinação especificada no documento, inclusive.

Considerando que a privacidade e a intimidade constituem direitos da personalidade de natureza extrapatrimonial, marcados, sobremaneira, pela intransmissibilidade e oponibilidade *erga omnes*, sua violação demanda a devida reparação pecuniária.

Conforme sustenta Schreiber (2014), o dano moral assume aqui uma função ambivalente: atua como instrumento de tutela compensatória para a vítima e exerce um caráter pedagógico-punitivo para o ofensor. No contexto do paciente, tal reparação integra seu patrimônio jurídico sem, contudo, transmutar a essência existencial do direito violado. Essa resposta jurídica é o que garante a eficácia da autodeterminação informativa, pois assegura que a falha estatal ou institucional no dever de proteção não permaneça sem a devida sanção, reafirmando a proteção de dados como um núcleo inviolável da dignidade humana.

À luz da concepção contemporânea que identifica a privacidade como direito fundamental à proteção de dados pessoais, eventual violação deve ser examinada sob a perspectiva da tutela da personalidade e não da propriedade, afirmando-se como expressão da autodeterminação informativa e como dimensão indissociável do livre desenvolvimento da personalidade, funcionando como mecanismo de contenção de discriminações, mercantilização indevida e exploração ilícita de dados sensíveis, servindo como instrumento contra discriminação, comercialização e divulgação indevida e ilícita dos dados pessoais e sensíveis dos pacientes.

CONSIDERAÇÕES FINAIS

Diante do exposto, conclui-se que o dever de confidencialidade médica, enquanto princípio basilar da profissão e expressamente previsto no Código de Ética Médica, não se limita à atuação individual do profissional, assumindo, no contexto hospitalar contemporâneo, dimensão institucional. A proteção e o adequado armazenamento dos dados pessoais e sensíveis dos pacientes atendidos em hospitais públicos e privados constituem obrigação que recai sobre toda a estrutura de prestação dos serviços de saúde, impondo a todos os profissionais que, direta ou indiretamente, tenham acesso a essas informações o dever de observância dos padrões de segurança, sigilo e responsabilidade no tratamento dos dados.

Os materiais utilizados nessa pesquisa apontam para o entendimento de que a utilização de simples termo de consentimento assinado pelo usuário do hospital não é suficiente para resguardar a proteção da atuação médica, tampouco é documento garantidor de proteção de que as informações pessoais e dados sensíveis do paciente, em especial no que tange ao comércio ilegal desse conteúdo sigiloso.

A lei de Proteção de Dados (LGPD), embora não tenha sido efetivamente implantada, visto que existe grande dificuldade na fiscalização dos tratamentos dos dados pessoais e sensíveis de usuários de serviços, certo é que a tecnologia – cada vez mais moderna, deve ser utilizada para o benefício das pessoas, i.e., segurança e privacidade devem ser o foco do manuseio das informações e não o contrário, dado o princípio da boa-fé que regem as relações consumeristas, especialmente no contexto hospitalar, mas antes disso, e acima de tudo, do princípio da dignidade da pessoa humana, que fundamenta a existência dos Direitos Humanos, pano de fundo, pois, do Estado de Direito, impondo, finalmente, que a tecnologia e os sistemas de informação em saúde estejam a serviço do paciente.

REFERÊNCIAS

BEAUCHAMP, Tom L.; CHILDRESS, James F. **Principles of biomedical ethics**. 6 ed. Nova Iorque: Oxford University Press; 2009.

BRANDEIS, Louis; WARREN, Samuel. **The right to privacy**. Harvard Law Review, vol. 4, 1890.

BRASIL, **Constituição Federativa do Brasil de 1988**. Brasília, DF: Presidente da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 nov. 2023.

BRASIL, **Resolução CFM nº 1931/2009**. Código de Ética Médica. 13/04/2010. Disponível em: <https://portal.cfm.org.br/etica-medica/codigo-2010/#:~:text=0%20novo%20c%C3%B3digo%20foi%20publicado,13%20de%20abril%20de%202010.&text=Copyright%202022%20CFM>. Acesso em: 10 nov. 2023.

BRASIL, Superior Tribunal de Justiça. **LGPD: Aplicação da Lei de Proteção Geral de dados no STJ**. Jun. 2023. Disponível em: <https://www.stj.jus.br/sites/portallp/SiteAssets/Paginas/Leis-e-normas/cartilha-lgpd.pdf>. Acesso em: 10 nov. 2023.

BRASIL. Lei 13.709/2018. **Lei Geral de Proteção de Dados**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2023.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. Tradução de Roneide Venancio Majer. 20. ed. São Paulo: Paz e Terra, 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJL], [S.l.], v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 14 jan. 2024.

DONEDA, Danilo. **A tutela da privacidade no Código Civil de 2002**. Grupo Educacional Opet. Disponível em: <https://www.opet.com.br/faculdade/re>

vista-anima/pdf/anima1/artigo_Danilo_Doneda_a_tutela.pdf. Acesso em: 14 jan. 2024.

FARIA, Paula Lobato de.; CORDEIRO, João Valente. **Health data privacy and confidentiality rights: Crisis or redemption?** Revista Portuguesa de Saúde Pública, v. 32, n. 2, p. 123-133, jul. 2014. Disponível em: <http://dx.doi.org/10.1016/j.rpsp.2014.10.001>. Acesso em: 14 jan. 2024.

FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Revista da Faculdade de Direito, Universidade de São Paulo, [S.l.], v. 88, p. 439-459, 1993. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/67231>. Acesso em: 14 jan. 2024.

KIRIMLIOGLU, Nurdan. **The right to privacy and the patient views in the context of the personal data protection in the field of health.** Biomedical Research, v. 28, n. 4, p. 1464-1471, 2017. Disponível em: https://www.researchgate.net/publication/326058221_The_right_to_privacy_and_the_patient_views_in_the_context_of_the_personal_data_protection_in_the_field_of_health. Acesso em: 14 jan. 2024.

LIPOVETSKI, Gilles. **Os tempos hipermodernos.** Trad. Mário. Vilela. São Paulo: Editora Barcarola, 2004.

LUIZON, Andressa Sanchez Silva Luizon. **Saúde Mental: uma reflexão sobre a internação psiquiátrica.** - 1.ed. - Rio de Janeiro: Lumen Juirs, 2025. ISBN 978-85-519-3778-5.

MORAES, Maria Celina Bodin de. **Ampliando os direitos de personalidade.** In: MORAES, Maria Celina Bodin de. **Na medida da pessoa humana: estudos de direito civil-constitucional.** Rio de Janeiro: Renovar, 2010.

OHM, Paul. **Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.** Revista SSRN, v. 57, p. 1701-1777, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 10 nov. 2023.

PAIANO, Daniela Braga. **Direito à intimidade e à vida privada.** Nov. 2003. Disponível em: <https://www.diritto.it/archivio/1/21084.pdf>. Acesso em: 14 jan. 2024.

ROBL FILHO, Ilton Norberto. **Direito, intimidade e vida privada: uma perspectiva histórico-política para uma delimitação contemporânea.** Rev Electrónica do CEJUR, v. 1, p. 184-205, 2006. Disponível em: https://www.researchgate.net/publication/228639869_Direito_Intimidade_e_Vida_Privada_uma_perspectiva_historico-politica_para_uma_delimitacao_contemporanea. Acesso em: 20 fev. 2024.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

STELZER, Joana. **O fenômeno da transnacionalização da dimensão jurídica**. In: CRUZ, Paulo Márcio; STELZER, Joana (org.). **Direito e transnacionalidade**. Curitiba: Juruá, 2009.

VILLAS-BÔAS, Maria Elisa. **O direito-dever de sigilo na proteção ao paciente**. *Rev. Bioética*, v. 23, n. 3, p. 513-523, 2015. Disponível em: <https://doi.org/10.1590/1983-80422015233088>. Acesso em: 20 fev. 2024.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. *Harvard Law Review*. Vol. 4, No. 5, p. 193-220, 15 dez. 1890. Disponível em: <https://www.gutenberg.org/files/37368/37368-h/37368-h.htm>. Acesso em: 20 fev. 2024.

Contato dos autores/as:

autor: Cláudio José Franzolin
e-mail: cfranzol30@gmail.com

autora: Andressa Sanchez Silva Luizon
e-mail: andressaluizon@yahoo.com.br

Manuscrito aprovado para publicação em: 05/02/2026.