Reciis – Revista Eletrônica de Comunicação, Informação & Inovação em Saúde, Rio de Janeiro, v. 17, n. 4, p. 938-961, out.-dez. 2023
[www.reciis.icict.fiocruz.br] e-ISSN 1981-6278

https://doi.org/10.29397/reciis.v17iAhead-of-Print.3602

RELATOS DE EXPERIÊNCIA

A autodeterminação informativa como contexto normativo para elaboração de diretrizes para a construção de um Relatório de Impacto à Proteção de Dados Pessoais: a proposta de um modelo humanizador para a telemedicina

Informative self-determination as a normative context for the elaboration of guidelines for the Impact Report on Personal Data Protection: the proposal of a humanizing model for telemedicine

La autodeterminación informativa como contexto normativo para la elaboración de lineamentos para la construcción de un Informe de Impacto en Protección de Datos Personales: la propuesta de un modelo humanizador para la telemedicina

Marcelo Minghelli[1,a]
marcelo.minghelli@ufsc.br | https://orcid.org/0000-0002-5964-2441

Nathalia Berger Werlang[1,b]
nathalia.werlang@ufsc.br | https://orcid.org/0000-0003-0172-6025

Barbara Balbis Garcia[1,c]
babibalbis@gmail.com | https://orcid.org/0000-0003-4530-0974

[1] Universidade Federal de Santa Catarina, Departamento de Ciência da Informação. Florianópolis, SC, Brasil.

[a] Doutorado em Direito pela Universidade Federal do Paraná.
[b] Doutorado em Administração pela Universidade Federal de Santa Catarina.
[c] Graduação em Ciência da Informação pela Universidade Federal de Santa Catarina.

RESUMO

Apresentamos e discutimos a construção de um instrumento de *compliance* para tratamento de dados pessoais e dados pessoais sensíveis do Núcleo Telessaúde UFSC, com base na Lei Geral de Proteção de Dados Pessoais. Trata-se da elaboração de diretrizes para um Relatório de Impacto à Proteção de Dados Pessoais visando à preservação da dimensão humana do dado e à preservação de direitos. A pesquisa foi qualitativa e exploratória, tendo o relato de experiência como metodologia. O levantamento bibliográfico e a análise documental permitiram a investigação, realizada em 2022, de processos, etapas e fluxos do tratamento dos dados. A análise dos dados foi qualitativa, por comparação dos resultados com a legislação vigente e com a adequação ao princípio da autodeterminação informativa. Os resultados demonstraram que as propostas para o relatório contribuíram para um tratamento de dados mais adequado ao ordenamento jurídico e, consequentemente, mais humanizado.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; Relatório de Impacto à Proteção de Dados Pessoais; Autodeterminação informativa; Telemedicina; Relato de experiência.

ABSTRACT

We present and discuss the construction of a compliance instrument for the processing of personal data and sensitive personal data of the Telessaúde UFSC Center, based on the General Data Protection Law. It is a model for the elaboration of guidelines for the construction of an Impact Report on the Protection of Personal Data that collaborates to the preservation of the human dimension of data and the preservation of rights. The research was qualitative and exploratory, adopting experience report as methodology. Bibliographical research and documental analysis enabled the investigation of the processes, stages and flows of data processing, carried out in 2022. Data analysis was carried out qualitatively, comparing the results with current legislation and adequacy to the principle of informative self-determination. Results showed that the proposed guidelines for the report contributed to a data processing more appropriate to the legal system and, consequently, more humanized.

Keywords: General Data Protection Law; Impact Report on the Protection of Personal Data; Informative self-determination; Telemedicine; Experience report.

RESUMEN

Presentamos y discutimos la construcción de un instrumento de cumplimiento para el tratamiento de datos personales y datos personales sensibles del Núcleo Telessaúde UFSC, con base en la Ley General de Protección de Datos. Es la preparación de directrices para un Informe de Impacto de Protección de Datos Personales para preservación de la dimensión humana de los datos y preservar los derechos. La investigación cualitativa y exploratoria adoptó un relato de experiencia como metodología. El levantamiento bibliográfico y el análisis documental permitieron la indagación de procesos, etapas y flujos de procesamiento de datos, realizados en 2022. El análisis de datos fue cualitativa, mediante la comparación de los resultados con la legislación vigente y la adecuación al principio de autodeterminación informativa. Los resultados mostraron que las directrices propuestas para el informe contribuyó a un tratamiento de datos más adecuado al ordenamiento jurídico y, en consecuencia, más humano.

Palabras clave: Ley General de Protección de Datos; Informe de Impacto de la Protección de Datos Personales; Autodeterminación informativa; Telemedicina; Informe de experiencia.

INFORMAÇÕES DO ARTIGO

Contribuição dos autores:
Concepção e desenho do estudo: Marcelo Minghelli.
Aquisição, análise ou interpretação dos dados: Marcelo Minghelli e Barbara Balbis Garcia.
Redação do manuscrito: Marcelo Minghelli e Nathalia Berger Werlang.
Revisão crítica do conteúdo intelectual: Nathalia Werlang.

Declaração de conflito de interesses: não há.

Fontes de financiamento: não houve.

Considerações éticas: não há.

Agradecimentos/Contribuições adicionais: não há.

Histórico do artigo: submetido: 23 fev. 2022 | aceito: 29 maio 2023 | publicado: 12 set. 2023.

Apresentação anterior: não há.

INTRODUÇÃO

A chegada dos dispositivos digitais e o aumento da conectividade resultaram em inúmeras mudanças no comportamento da sociedade (Leonardi; Treem, 2020). Diante disso, a adoção de recursos, a exemplo do Big Data e da Internet das Coisas (IoT), está cada vez mais presente no dia a dia pessoal e profissional da humanidade, o que gera oportunidades, mas também desafios (Davenport, 2014).

Toda essa transformação cunhou a valorização dos dados como o principal recurso de um ambiente organizacional, aumentando a necessidade de as organizações adquirirem esses dados, contribuindo, dessa forma, para o aumento da competitividade. Essa nova era trouxe consigo o conceito de capitalismo de vigilância, que, de acordo com Zuboff (2019), pode ser definido como uma nova realidade social com diferentes interações por meio de mídias e dispositivos altamente conectados. No capitalismo de vigilância, o acúmulo de dados pessoais, a partir das plataformas digitais, é a todo momento processado e permite que as organizações iniciem um processo de mercantilização desses dados (Kellogg; Valentine; Christin, 2020; Zuboff, 2019).

Esse novo contexto nos serve de base para a reflexão acerca do princípio da autodeterminação informativa, que tem como elemento normatizador o tratamento de dados. A questão é complexa e transcende a mera positivação de valores no ordenamento jurídico nacional, incidindo na dimensão dogmática do direito e na dimensão da ciência da informação como ciências sociais aplicadas.

A autodeterminação informativa é um dos fundamentos da disciplina de proteção de dados pessoais. Ela parte do princípio de que o tratamento de dados deve ocorrer apenas quando há uma justificativa legal, a partir da finalidade do processamento (Mendes, 2020).

É possível relacionar esse cenário com as provações de Harari (2016), que propõe um questionamento acerca dos resultados de três macroprocessos interconectados que, em suma, estabelecem: 1) que a ciência, atualmente, desenvolve uma face dogmática ao resumir a vida ao processamento de dados e os organismos vivos aos algoritmos; 2) que a inteligência está se desconectando da consciência e; 3) que os algoritmos poderão, em breve, conhecer os indivíduos melhor que eles mesmos.

Esses processos, quando alcançassem seu ápice, levariam a humanidade a substituir a visão 'antropocêntrica' da vida por uma visão 'datacêntrica', retirando o protagonismo do indivíduo e resumindo a sua existência ao papel que ele desempenha nos infindáveis mecanismos de processamento de dados. Como Harari define: "[...] um pequeno *chip* dentro de um sistema gigantesco que, na realidade, ninguém entende" (Harari, 2016, p. 388). Dessa forma, o indivíduo só encontraria significado para a sua existência enquanto participante desse fluxo interminável de dados, fosse ao responder a *e-mails*, ao escrever artigos, ou mesmo ao compartilhar fotos e experiências ao infinito. Sendo assim, a experiência só tem sentido na medida em que contribui para a troca global de informações, mas sem a consciência desse intenso processo informacional.

Evidencia-se, então, que a dimensão humana do dado e, por consequência da informação, é, no mínimo, diminuída ou mesmo subtraída. O tratamento seria concebido como um fluxo informacional, relativizando os milhares de fragmentos da personalidade humana que nele estão inseridos e são constantemente manipulados. A objetificação da personalidade humana, nessa conjuntura, traz desafios de ordem filosófica, científica e tecnológica. Não se trata apenas de normatizar o tratamento de dados ou de criar novas formas de gerenciar e processar o imenso universo de informações por ele disponibilizadas, mas de preservar a dimensão humana.

Assim, a preservação dessa dimensão humana começa a ser desenhada com a adoção do princípio da autodeterminação informativa, que, mesmo antes da vigência da Lei Geral de Proteção de Dados Pessoais (LGPD), impunha ao tratamento de dados um '*know-how* ético', uma espécie de orientador que objetiva

garantir ao indivíduo um mínimo de consciência ou controle das informações que sobre ele circularam na sociedade contemporânea.

Na tentativa de operacionalizar esse princípio, a equipe do Núcleo Telessaúde UFSC elaborou um modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), tendo como centralidade a dimensão humana do tratamento, ou seja, o titular de dados.

Por mais óbvio que pareça, não são raros os exemplos de práticas de implantação da nova legislação (LGPD) que se materializam tendo como prioridade as empresas e instituições, limitando suas atividades de *compliance*[1] ao mínimo necessário para evitar riscos indenizatórios ou multas.

Diante da contextualização, este artigo tem como objetivo apresentar e discutir as diretrizes para a construção de um RIPD que colabore para a preservação da dimensão humana do dado, sem prescindir da ligação à personalidade do indivíduo e da necessidade de preservação de direitos.

Espera-se que os achados deste estudo possam contribuir para o avanço teórico da temática, que ainda é incipiente e necessita ampliar as discussões acerca da LGPD e do RIPD. Além disso, espera-se contribuir para a prática das organizações que precisam se adaptar à nova realidade da gestão dos dados pessoais e aos devidos fluxos de tratamento, bem como à importância da elaboração do RIPD.

AUTODETERMINAÇÃO INFORMATIVA, LGPD E RIPD

O indivíduo, na sociedade contemporânea, perde facilmente a centralidade de sua existência no emaranhado e no intenso fluxo de dados e informações.[2] Torna-se incapaz de dar sentido à sua própria existência, de ter domínio sobre as suas próprias experiências, ao perder o controle total de como é visto e entendido. As novas tecnologias e os artefatos que vêm com ela têm influenciado e reconfigurado o ambiente organizacional (Davenport, 2014), assim como a privacidade das pessoas e as relações que elas estabelecem entre si (Zuboff, 2019).

Esse novo contexto social, que engloba diferentes relações e interações por meio de mídias e dispositivos digitais interconectados, é o que se chama de capitalismo de vigilância – termo cunhado por Zuboff (2019). O conceito de capitalismo de vigilância é representado por um sistema tecnológico, que integra indivíduos, suas relações e seus comportamentos, mediado por plataformas digitais, que, posteriormente, são gerenciadas por algoritmos (Kellogg; Valentine; Christin, 2020; Leonardi; Treem, 2020; Zuboff, 2019).

Grandes organizações que atuam com serviços digitais acabam exercendo poder pela forma com que fazem a gestão e se relacionam com outros atores, a exemplo dos usuários, com outras organizações e também com o Estado. Isso ocorre pelo fato de elas coletarem diferentes tipos de dados, oriundos de comportamentos e interações nas redes sociais (Leonardi; Treem, 2020). Dessa forma, o indivíduo, entendido como pessoa natural, torna-se objeto dos tratamentos de dados, e as dimensões de sua vida e personalidade são absorvidas nesse fluxo informacional como dados.

Como expõe Frazão (2019), atualmente os algoritmos são projetados para extrair informações sobre padrões de comportamento e realizar inferências acerca dos indivíduos, para que posteriormente seja

1 Ato de estar de acordo com as normas, leis e regulamentações vigentes.

2 O conceito de dado e o conceito de informação podem ser apresentados em diferentes dimensões, conforme a área do conhecimento e o conjunto de autores com que se analisam as referidas categorias. Para os objetivos desta reflexão, opta-se pela dimensão oferecida pela dogmática jurídica nacional, por dois motivos. O primeiro é que a centralidade das reflexões apresentada se refere ao impacto dos regimes informacionais sobre os indivíduos e o desenvolvimento autônomo de suas personalidades. O segundo é a própria assimilação do princípio na autodeterminação informativa como elemento normatizador ou critério valorativo de um regime informacional. Nesse sentido, o artigo 5º, inciso I, da Lei Geral de Proteção de Dados Pessoais (LGPD – lei n. 13.709/2018) define dado pessoal como toda e qualquer informação relacionada a uma pessoa natural identificada ou identificável, enquanto o artigo 4º, inciso I da Lei de Acesso à Informação (lei n. 12.527/2011) define que a informação é um conjunto de dados tratados ou não usados para a produção ou transmissão de conhecimento. Para a presente reflexão interessa a transversalidade da LGPD, ou seja, o elemento essencial é o elemento humano, na medida em que o dado ou a informação se refere a uma pessoa natural, ou seja, a um ser humano, independentemente da carga cognitiva que esse dado ou essa informação possa trazer.

possível tomar decisões sobre questões objetivas e subjetivas, por meio da coleta de dados sensíveis. Alguns exemplos são: avaliar características pessoais sobre personalidade dos indivíduos, mapear o estado de atenção, estados emocionais e pensamentos, identificar habilidade para determinadas funções, avaliar indicativos de criminalidade, prever doenças, entre outros.

Face a esta nova configuração, a resposta das instituições típicas do Estado moderno, como o Parlamento e o Judiciário, foi a institucionalização do princípio da autodeterminação informativa. Uma tentativa de proteger o indivíduo no contexto atual de produção informacional caracterizado pelo capitalismo de vigilância, que o objetifica e que invade o núcleo de sua personalidade, cujas consequências ainda não são totalmente conhecidas.

O princípio da autodeterminação informativa é uma reação da matriz axiológica, típica da modernidade, aos processos de objetificação do ser humano produzidos pelos diferentes regimes informacionais estabelecidos por atores econômicos e estatais. Esse princípio se constitui numa proteção dinâmica das dimensões da personalidade do ser humano, atribuindo-lhe, na dimensão jurídica, o controle sobre as suas próprias informações (Rodotà, 2008), transcendendo a dicotomia entre o público e o privado, ao mesmo tempo que institui um parâmetro axiológico e avaliativo para a análise dos regimes de informação estabelecidos.

Não é por acaso que a autodeterminação informativa surge em duas decisões paradigmáticas do Supremo Tribunal Federal (STF), fazendo menção explícita à relação umbilical entre as garantias constitucionais da liberdade individual, da privacidade e do livre desenvolvimento da personalidade (artigo 5º, *caput* e incisos X e XII) e a lei de n. 13.709/2018 (LGPD), que positivou o princípio em seu artigo 2º, inciso II. Nesse sentido, seguiu a tradição do Tribunal Constitucional Federal alemão, que, em 1983, consagrou a autonomia do referido princípio ao declarar a inconstitucionalidade da Lei do Censo alemã.

A primeira decisão, a Arguição de Descumprimento de Preceito Fundamental n. 722, foi interposta pela Rede Sustentabilidade, em face da atividade de inteligência do Ministério da Justiça e Segurança Pública na produção e disseminação do dossiê com informações de servidores federais e estaduais integrantes do movimento antifascismo (Brasil, 2020c).

O acórdão do STF determinou a suspensão imediata das atividades do referido ministério que estabeleciam a produção ou o compartilhamento de informações pessoais sobre os servidores que integravam o movimento antifascista. No voto da ministra Rosa Weber, verifica-se a menção ao princípio da autodeterminação informativa como decorrente dos direitos de personalidade e cita-se:

> Com efeito, informações relacionadas à identificação – efetiva ou potencial – de pessoa natural, como as alegadamente contidas no documento em questão, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. Em estreita consonância com as cláusulas protetivas dos direitos e garantias individuais consagrados na Constituição da República, o art. 5º, II, da Lei Geral de Proteção de Dados Pessoais (lei n. 13.709/2018) classifica, ainda, como dados sensíveis as informações pessoais atinentes à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual de uma pessoa natural, bem como seus dados genéticos ou biométrico (Brasil, 2020c).

A segunda decisão é ainda mais veemente ao estabelecer o princípio da autodeterminação informativa. A Ação Direta de Inconstitucionalidade n. 6.387 foi ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) em face da medida provisória n. 954/2020, que estabelecia o compartilhamento de

dados dos usuários do serviço telefônico fixo e móvel pelas empresas prestadoras de serviço com o Instituto Brasileiro de Geografia e Estatística (IBGE) (Brasil, 2020a). Nesse caso, o princípio da autodeterminação informativa é utilizado na motivação apresentada no acórdão na quase totalidade dos votos apresentados pelos ministros da Corte Constitucional.

A decisão do STF vai além da mera menção: declara que a autodeterminação informativa decorre dos direitos de personalidade, como o direito à privacidade, trazendo como impacto a sua obrigatória observância a qualquer regime informacional. Em outras palavras, os dados pessoais e os dados pessoais sensíveis não são e nunca poderão ser propriedade ou meros objetos de tratamento de dados em amplo sentido. Eles estão ligados à personalidade de seus titulares, pessoas naturais, de forma inalienável, gerando um rol de obrigações jurídicas para os atores econômicos, estatais e sociais que os tratem ou manipulem em qualquer dimensão.

A natureza autônoma e ligada aos direitos de personalidade perpassa toda a decisão emitida pela Suprema Corte, o que, por si só, já mereceria análise em trabalho específico. Mas, para fins desta reflexão, são destacadas algumas passagens, entre elas a manifestação do ministro Luiz Fux (Brasil, 2020b, p. 8):

> A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do *habeas data* (art. 5º, LXXII), todos previstos na Constituição Federal de 1988.

No contexto nacional, muito embora a LGPD traga a autodeterminação informativa como um de seus fundamentos expressos no inciso II do artigo 2º (Brasil, 2018), e a sua promulgação tenha sido acompanhada de grande interesse por parte da sociedade, faz-se necessário afirmar que se trata de direito autônomo já consagrado pelo ordenamento jurídico nacional tanto na *Carta Magna* como na legislação infraconstitucional.

No voto do ministro Gilmar Mendes pode-se destacar a assimilação do processo ocorrido pela Corte Constitucional alemã, que se tornou o marco histórico do princípio da autodeterminação informativa. Cita-se (Brasil, 2020c, p. 13):

> Essa abertura da jurisdição constitucional à transformação tecnológica enquanto instrumento de preservação dos direitos fundamentais também é consolidada na tradição continental. No icônico precedente da Lei do Censo alemã de 1983, cuja análise será aprofundada neste voto, resta evidente que o avanço das técnicas de coleta e processamento de dados foi tomado como válvula de reconfiguração da proteção jurídica à personalidade. A decisão baseou-se principalmente no diagnóstico de que, a partir da coleta e cruzamento de dados do censo, "seria possível a criação de um quadro abrangente e detalhado da respectiva pessoa, um perfil de personalidade, mesmo na área íntima; o cidadão torna-se uma verdadeira 'pessoa transparente'".

O ministro traça ainda um quadro evolutivo e comparativo da tradição da *common law* com o precedente da Corte Constitucional alemã, passando pela doutrina nacional, sem deixar de citar o artigo The right to privacy, de Samuel Warren e Louis Brandeis, fundamental para a percepção de que o direito à privacidade se desvincula do direito à propriedade, integrando-se ao rol de direitos de personalidade em uma dimensão autônoma.

> Essa nova abordagem revelou-se paradigmática por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso. Como bem destacado na decisão, a identificação de um constante avanço tecnológico demanda igualmente a afirmação de um direito de personalidade que integre o contexto das "condições atuais e

> futuras circunstâncias do processamento automático de dados" (*heutigen und künftigen Bedingungen der automatischen Datenverarbeitung*). É justamente essa reconfiguração que possibilita a afirmação do direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo (Brasil, 2020c, p. 19).

Em síntese, o princípio da autodeterminação informativa estabelece um critério de legitimidade jurídica para o tratamento de dados na contemporaneidade. Os diferentes atores, processos, tecnologias e regras organizacionais devem obrigatoriamente respeitar os limites desse princípio que reafirma a centralidade do indivíduo titular dos dados e das informações, afastando concepções que tratem os dados pessoais como meras *commodities*, objetos científicos ou meros dados estatísticos, entre outras concepções possíveis.

O RIPD não pode fugir desse contexto normativo estabelecido pelo princípio da autodeterminação informativa. Um princípio não só incorporado pela emenda constitucional n. 115/2022, mas pela própria atividade jurisdicional nacional e internacional, como vimos anteriormente. Nesse sentido, embora o RIPD não tenha sido completamente regulamentado e pairem sobre ele dúvidas em diferentes dimensões[3], ele é hoje considerado um instrumento indispensável à autodeterminação informativa.

É através do RIPD que os agentes de tratamento irão prestar contas da utilização dos dados pessoais, obrigando-os a uma reflexão contínua de suas práticas, levando em conta que esses dados estão, perenemente, conectados à essência humana. Assim, a sua obrigatoriedade e a sua publicização são uma questão de tempo até o amadurecimento da legislação infraconstitucional.

METODOLOGIA DA PESQUISA

No estudo propomos apresentar e discutir a construção de um instrumento de controle para que os agentes de tratamento considerem a dimensão humana do dado pessoal, sua ligação à personalidade dos titulares e a necessidade de preservação dos direitos dos titulares.

As escolhas metodológicas que adotamos partiram dos pressupostos de uma pesquisa qualitativa e exploratória, uma vez que investigamos uma temática ainda incipiente na academia e que necessita de mais aprofundamento (Mattar, 2001).

Além disso, a pesquisa é caracterizada como teórica-empírica, visto que foram coletados dados primários e secundários para o alcance do objetivo proposto. A estratégia metodológica adotada foi o relato de experiência, que parte de uma perspectiva social (Minayo, 2001).

Este relato de experiência compreende um período de trabalho que vai de março de 2022 a outubro de 2022, realizado por um grupo de pesquisadores multidisciplinar das áreas do direito, da ciência da informação e da arquivologia.

Os dados secundários – documentos e resoluções relacionados ao tema; artigos científicos; modelos de relatórios de impacto publicados por outras organizações; informações do Núcleo Telessaúde UFSC – foram coletados e obtidos a partir da página oficial do programa disponibilizada na internet.

Os dados primários foram coletados por meio do acesso ao processo de tratamento de dados estabelecido pelo Núcleo Telessaúde UFSC, com análises dos fluxos, verificação dos dados coletados, periodicidade de coleta e forma de tratamento.

A etapa do levantamento dos dados utilizados pelo Núcleo Telessaúde UFSC foi realizada a partir da análise do volume dos dados dos projetos constitutivos do núcleo: teleconsultoria e telediagnóstico.

3 Como afirma Gomes (2021), os principais desafios para a regulamentação do RIPD são: "[...] (i) [a] definição da ferramenta e objetivo da função do relatório no contexto da LGPD; (ii) o conceito de risco, análise e documentação necessária; (iii) a obrigatoriedade de elaboração; (iv) a metodologia para elaboração do relatório; e (v) o estabelecimento de parâmetros, a prestação de contas e sua publicização".

Posteriormente foi investigado o organograma que representa a cadeia hierárquica e as relações de todas as áreas envolvidas no Núcleo do Telessaúde UFSC.

Para a construção do RIPD procedemos da seguinte maneira: no primeiro momento, analisamos o volume de dados, o organograma dos agentes de tratamento de dados envolvidos e os fluxos do tratamento de dados realizados nos projetos constitutivos do núcleo: Telediagnóstico, Teleconsultoria e Tele-Educação.

Na segunda etapa, os dados tratados foram classificados de acordo com a legislação e a doutrina jurídica nacional em três categorias básicas: dados, dados pessoais e dados pessoais sensíveis. De forma concomitante, levantamos a finalidade e o propósito de uso de cada dado tratado e o perfil de seus titulares, bem como analisamos a necessidade e a proporcionalidade de cada dado tratado e a sua relação de adequação com a LGPD.

A primeira e a segunda etapas, consideradas de diagnóstico geral, permitiram uma ampla visão do tratamento de dados executado. Ambas foram fundamentais para a identificação de eventuais riscos, bem como para a atribuição do nível de gravidade e urgência para cada possível incidente. As atividades da terceira e da quarta etapas, realizadas concomitantemente, têm por objetivo estabelecer a relação entre os riscos e os direitos dos titulares.

Na quinta e última fase, elaboramos um conjunto de medidas para dar respostas aos eventuais riscos, atribuindo responsabilidades de execução, urgência na execução e data para a sua efetivação. Todas as medidas foram elaboradas para dar ao titular mais controle e informações sobre os seus dados, obedecendo ao princípio da autodeterminação informativa, além de possibilitar maior conformidade às etapas do tratamento efetivado.

A etapa de análise dos dados deu-se de maneira qualitativa, por meio de uma comparação dos resultados com a legislação vigente. Foram abordados, inicialmente, os aspectos gerais da LGPD, o tratamento de dados sensíveis e a confidencialidade na área da saúde. Por fim, o trabalho apresenta os aspectos utilizados para a construção do RIPD.

As técnicas aqui empregadas nos permitiram obter maior conhecimento acerca do tema investigado e, assim, descrever as etapas utilizadas para o desenvolvimento de um RIPD com base nas normatizações e também no que é executado na prática da unidade analisada.

Este relato foi escrito pelos pesquisadores que realizaram o trabalho. Dessa forma, foram tomados todos os cuidados necessários para a apresentação das etapas desenvolvidas durante o processo de coleta e desenvolvimento do relatório. Entretanto, o processo de construção coletivo pode apresentar reflexões e posicionamentos inerentes aos pesquisadores envolvidos nesse percurso (Minayo, 2001).

A seguir será apresentado um breve relato do Núcleo Telessaúde UFSC, a fim de contextualizar os leitores acerca do objeto de estudo do artigo.

A DESCRIÇÃO DO NÚCLEO TELESSAÚDE UFSC E O VOLUME DE DADOS

O Núcleo Telessaúde UFSC é parte integrante do Programa Nacional Telessaúde Brasil Redes, do Ministério da Saúde (MS), e se materializa em projetos de extensão da Universidade Federal de Santa Catarina com objetivo de executar políticas públicas que implementem e qualifiquem o acesso ao direito fundamental à saúde inscrito na *Carta Magna*, conforme artigos 6º e 196 da Constituição Federal (Brasil, 1988).

Assim, todas as atividades desenvolvidas, direta ou indiretamente, buscam a tutela da saúde, seja nas atividades de suporte e formação dos profissionais, seja na oferta de serviços aos usuários do Sistema Único de Saúde (SUS). As atividades compõem, desde 2010, o Sistema Integrado Catarinense de Telemedicina e Telessaúde (STT).

Os serviços do Núcleo Telessaúde consistem em:

I) Teleconsultoria: consulta registrada e realizada entre trabalhadores, profissionais e gestores da área da saúde, por meio de instrumentos de telecomunicação bidirecional, com objetivo de esclarecer dúvidas sobre procedimentos clínicos, ações de saúde e questões relativas ao processo de trabalho, com respostas baseadas em evidências científicas e adequadas às características locorregionais.

São tipos de teleconsultoria: a) Teleconsultoria clínica: objetiva esclarecer dúvidas sobre o manejo, as condutas e os procedimentos clínicos no escopo da Atenção Básica/Atenção Primária à Saúde (APS); b) Teleconsultoria de processo de trabalho/coordenação/gestão: fornece suporte aos profissionais da rede de APS do SUS no que se refere à organização do trabalho no contexto da Atenção Básica, por meio de consulta a um especialista (teleconsultor) em Saúde da Família/Saúde Coletiva; e c) Teleconsultoria com intenção de encaminhamento: consiste na análise e discussão de um caso, com o objetivo de auxiliar o profissional responsável a encaminhar o referido caso à especialidade de referência. A teleconsultoria é executada em dois formatos: teleconsultoria síncrona e teleconsultoria assíncrona.

II) Telediagnóstico: tem como objetivo primário facilitar o acesso do cidadão aos resultados de exames e laudos por meio do STT, bem como disponibilizar informações ao médico requisitante, ao médico executor e aos profissionais de saúde para melhor atender ao paciente.

III) Tele-Educação: desenvolve atividades de formação permanente e continuada de profissionais da área de saúde com o objetivo de promover, permanentemente, reflexão e avaliação dos processos de trabalho e das práticas de saúde. São atividades do Tele-Educação: a) webpalestras; b) webseminários; c) fóruns de discussão, d) reuniões de matriciamento; e e) cursos à distância.

Em 2016, foram realizados cerca de 6.500 atendimentos em teleconsultoria síncrona e assíncrona. Os casos mais relevantes e de maior frequência são enviados para a Biblioteca Virtual em Saúde (BVS), após seleção, análise, revisão e embasamento bibliográfico realizados pelo grupo de teleconsultores. Atualmente, existem cerca de 70 teleconsultorias publicadas na BVS.

Em 2021, foram realizados mais de 10 milhões de exames com o auxílio de tecnologias e do STT. Os profissionais da saúde e os usuários do SUS dos municípios de Santa Catarina tiveram acesso a esses exames de forma segura, rápida e sem necessidade de deslocamentos, o que aumenta a eficiência dos serviços e amplia o acesso ao direito fundamental à saúde.

Desde 2009, o Tele-Educação já obteve mais de 76 mil participações em webpalestras, 1.500 alunos foram certificados à distância nos minicursos oferecidos desde 2010 e, atualmente, estão disponibilizadas cerca de 1.000 webpalestras aos profissionais da saúde.

Pode-se verificar, portanto, que as atividades do Núcleo Telessaúde UFSC caracterizam-se como uma política pública fundamental para o acesso e a democratização a serviços de saúde.

Nesse contexto, os dados de profissionais da área de saúde e de usuários do SUS são tratados em volume significativo. Destaca-se, ainda, que parte expressiva dos dados é caracterizada como dados pessoais sensíveis, gerando a necessidade de implementação de processos e políticas internas que assegurem o cumprimento de normas e boas práticas relacionadas aos direitos dos titulares de dados tratados pelo núcleo.

PRIMEIRA ETAPA: ORGANOGRAMA, VOLUME DE DADOS E FLUXOS

Ao iniciar as atividades, efetuamos um diagnóstico geral do tratamento de dados realizado. O primeiro aspecto analisado, de fundamental importância para a elaboração do RIPD, é o organograma dos sujeitos envolvidos no tratamento.

O organograma identifica a função de cada ator envolvido no tratamento de dados e suas atribuições. Sem um organograma bem constituído seria muito difícil identificar os agentes de tratamento expressos nos incisos VI e VII, do artigo 5º, da LGPD e suas respectivas responsabilidades perante os órgãos de controle e os próprios titulares. A Figura 1 apresenta o organograma da equipe do Núcleo Telessaúde.

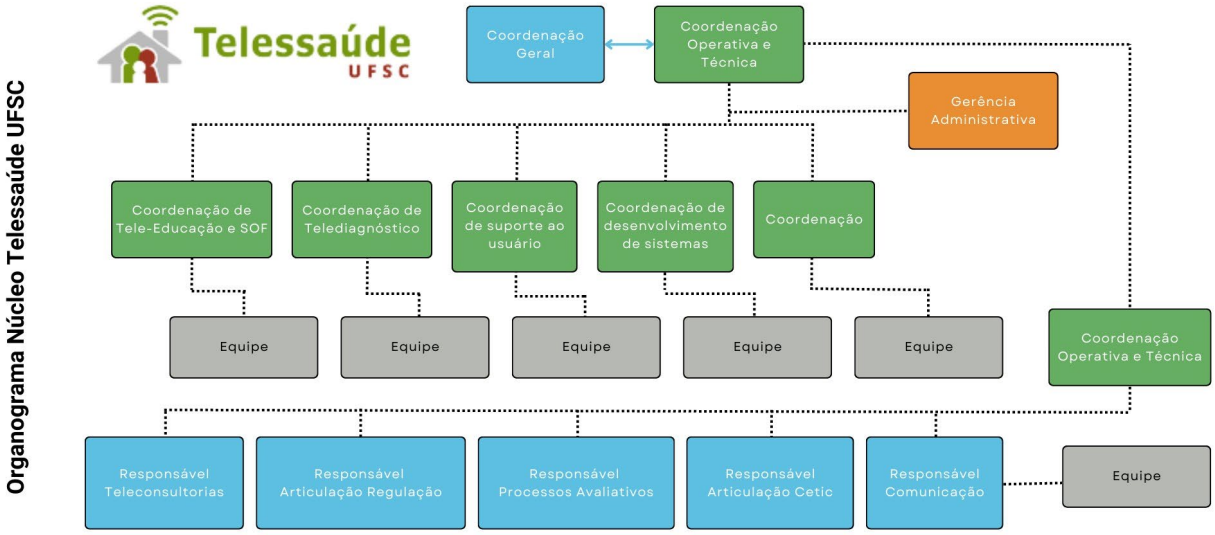

Figura 1 – Organograma do Núcleo Telessaúde UFSC
Fonte: Adaptada pelos autores a partir dos dados de Núcleo Telessaúde UFSC (2022).

Após a análise do organograma e a realização de entrevistas com os coordenadores do projeto, foi possível identificar os agentes de tratamento que são o controlador e o operador do Núcleo Telessaúde UFSC. Também foi possível verificar outros atores envolvidos no processo que dá acesso aos dados tratados e inserir esses profissionais na supervisão dos agentes de tratamento, observando-se suas respectivas atribuições.

A partir da análise e da descrição do programa, conforme apresentado no item 4 deste artigo, foi possível identificar um grande volume de dados no Núcleo Telessaúde UFSC. Esses dados serão posteriormente classificados e analisados para compor a próxima etapa de elaboração do RIPD descrita nas partes seguintes deste artigo.

Para a análise dos fluxos, a equipe de trabalho considerou a LGPD, que afirma que toda a operação realizada com dados pessoais é tratamento. O artigo 5º da LGPD define o ciclo de vida dos dados apontando as seguintes etapas de tratamento: 1) coleta/recepção, 2) produção/reprodução, 3) utilização, 4) acesso, 5) transmissão/distribuição, 6) transferência, 7) processamento, 8) arquivamento, 9) armazenamento, 10) eliminação, 11) avaliação, 12) controle da informação, 13) modificação, 14) comunicação e 15) difusão ou extração.

O relatório foi construído a partir da análise e da descrição de todos os fluxos de tratamento dos dados, iniciando-se pelo tratamento de dados por tipo de serviço. No que se refere ao Telediagnóstico, foram avaliados os fluxos de: autocadastro, solicitação de exames, envio de imagens para exame, emissão de laudo para exame, acesso ao exame, envio de dados dos exames ao MS e emissão de relatórios.

Ao avaliar o serviço Teleconsultoria, verificamos que este apresenta apenas um fluxo, o qual é iniciado quando um profissional assistente cria um pedido de apoio, descrevendo detalhadamente o caso, via STT, em área restrita. A seguir, o teleconsultor que atende o sistema, faz uma avaliação da demanda e gera uma resposta com recomendação de fluxo e conduta para profissional.

Por fim, para o serviço de Tele-Educação, foram apresentados os fluxos de autocadastro, o acesso às webpalestras, o acesso aos cursos no Moodle e o envio de indicadores de produção ao MS. Foram elaborados fluxogramas para cada processo, a fim de identificar o fluxo dos dados e os responsáveis pelo tratamento das informações.

Para todos os fluxos de cada um dos serviços do Núcleo Telessaúde foram criados fluxogramas dos processo e tratamento dos dados. A seguir, a Figura 2 apresenta como exemplo, o fluxograma do autocadastro do serviço Tele-Educação.

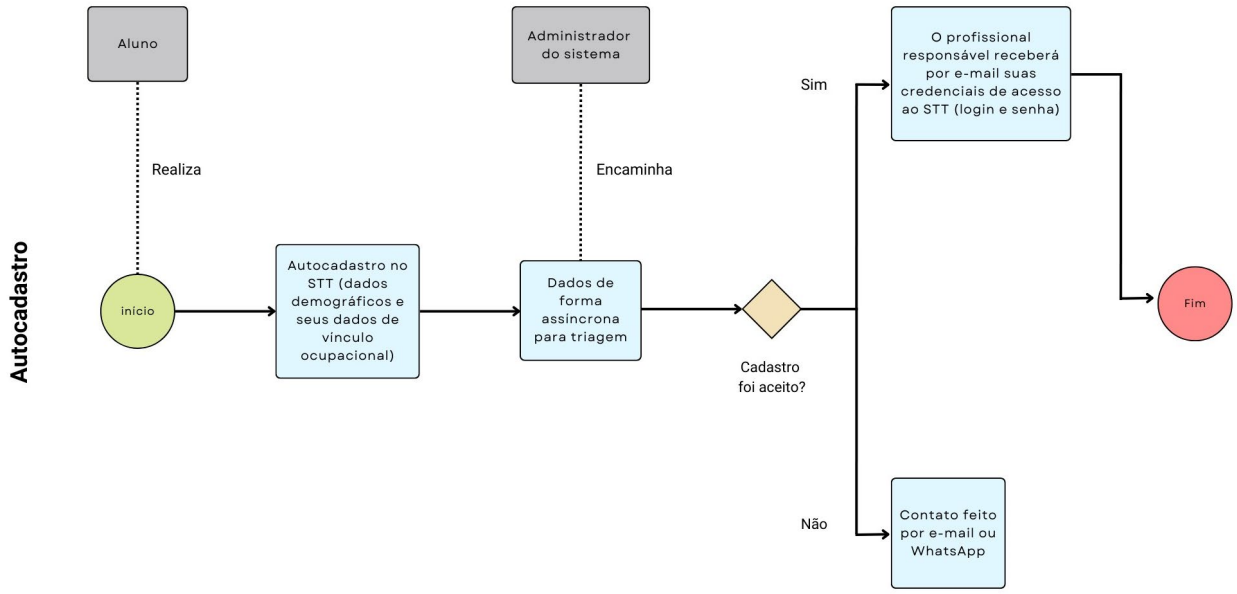

Figura 2 – Fluxograma de autocadastro – Tele-Educação
Fonte: Elaborada pelos autores.

Os atores mencionados na primeira caixa do fluxo procedem com seu autocadastro no STT, informando seus dados demográficos e vínculos ocupacionais. Por sua vez, o administrador do sistema encaminha esses dados, de maneira assíncrona, para a triagem. Nesse momento, o cadastro poderá ser rejeitado ou aceito sem modificações ou com correções/complementos, a partir de dados provenientes de cadastros disponibilizados pelo MS. Uma vez aceito o autocadastro, o profissional responsável por preenchê-lo receberá, via *e-mail*, suas credenciais de acesso ao STT (*login* e senha). Caso contrário, o solicitante receberá um *e-mail* ou WhatsApp.

Outro fluxo importante para a elaboração do RIPD é o do compartilhamento de dados. Esse fluxo permitirá a identificação de outras instituições no tratamento de dados, bem como suas atribuições na atividade, fundamental para mensurar os riscos ou mesmo apurar as responsabilidades futuras em eventuais incidentes.

A Figura 3 representa o compartilhamento de dados por meio de relatório emitido pelo módulo de Business Intelligence (BI), que gera diariamente uma cópia dos dados incrementais, a partir do banco de dados do STT, transformando-os em variáveis aplicáveis na geração de relatórios.

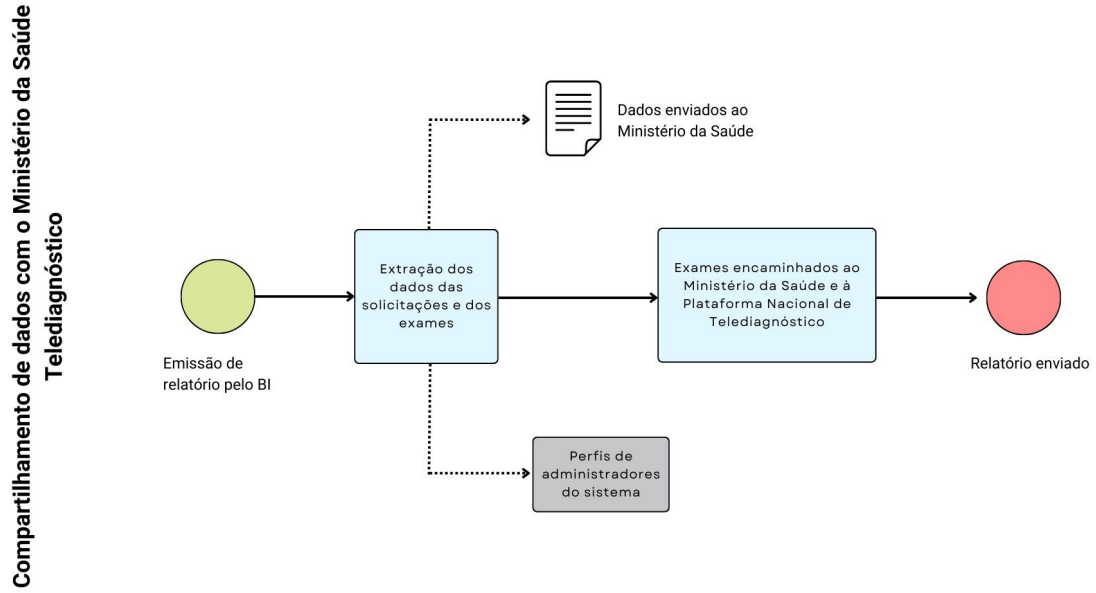

Figura 3 – Fluxograma de compartilhamento – Telediagnóstico
Fonte: Elaborada pelos autores.

Por se tratar de um programa do MS, há a necessidade de se comprovar a realização das atividades do Telediagnóstico. O ministério, como o gestor do programa, utiliza os dados tanto para o monitoramento do uso de recursos, quanto para a avaliação do impacto do programa no sistema de saúde – o que tende a auxiliar o planejamento de ações do Telessaúde no âmbito do SUS.

Assim, é de responsabilidade dos perfis administrativos do sistema a geração/emissão de tais relatórios (teleconsultores e coordenador de área do núcleo têm permissão para emitir os relatórios). A Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação (SeTIC) da UFSC é responsável pelo suporte do sistema de informação que sustenta as ações do Núcleo Telessaúde UFSC.

A Figura 4 representa o compartilhamento de dados dos indicadores de produção para o MS. A data para a extração dos dados finda no quinto dia útil do mês, quando são recuperados os dados referentes ao mês anterior, a partir do banco de dados do STT. Os dados são transformados e organizados de acordo com as especificações da plataforma de destino (plataforma Smart) e enviados via internet.

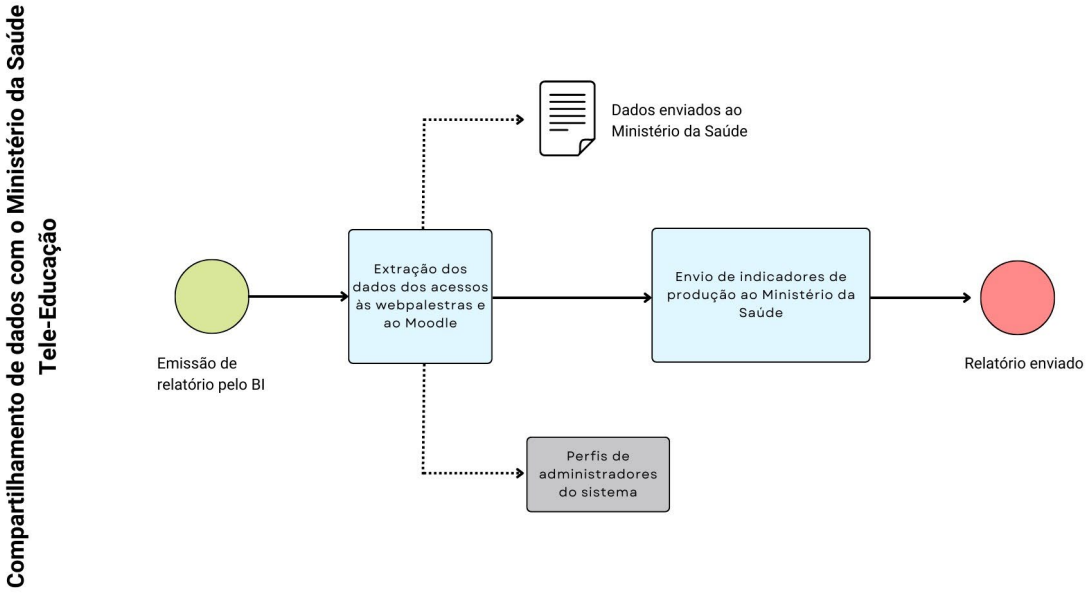

Figura 4 – Fluxograma de compartilhamento – Tele-Educação
Fonte: Elaborada pelos autores.

SEGUNDA ETAPA: CLASSIFICAÇÃO DOS DADOS, FINALIDADE E PROPÓSITO DE USO

Nessa etapa de classificação e análise da finalidade e do propósito de uso dos dados, nosso grupo de trabalho elencou todos os dados coletados para a realização das atividades, especificando suas finalidades e seu propósito de uso. Sobre a finalidade, a doutrina acerca da LGPD expõe a sua ligação umbilical com os princípios da adequação e necessidade, cuja aplicação conjunta indica a adoção da cultura da *Purpose limitation* (Limitação da finalidade).

Ainda sobre o propósito e a finalidade, cabe ressaltar que utilizamos para a construção desse relatório uma análise em diferentes dimensões, mas de forma simultânea. O propósito irá explicitar o escopo da coleta do dado para fins operacionais do projeto, e a finalidade será explicada pela base legal de tratamento nos termos dos artigos 7º e 11 da LGPD, expondo simultaneamente as dimensões fática e jurídica da finalidade.

Ao destacar a dimensão jurídica, tivemos por objetivo estabelecer maior alinhamento com o princípio da autodeterminação informativa, base axiológica da LGPD. O destaque facilita o entendimento, por parte dos agentes de tratamento, de que os dados são dos titulares e que, para tratá-los, deve haver, necessariamente, uma base de legitimidade jurídica, além de operacional.

A classificação foi realizada a partir de três categorias básicas – dado, dado pessoal e dado pessoal sensível – fornecidas pela legislação. Evidentemente, o termo 'dado', puro e simples, se refere ao dado anonimizado. A classificação também foi feita com base no perfil do titular: pacientes, profissionais da área de saúde e gestores.

Ao fim da análise dos dados cadastrais dos profissionais de saúde e gestores foi possível identificar que cem por cento desses dados solicitados são classificados como pessoais.

Em relação à proporcionalidade de dados relacionados aos pacientes foi possível observar que a maior parte dos dados solicitados é classificada como dados pessoais sensíveis. A Figura 5 apresenta esses resultados:

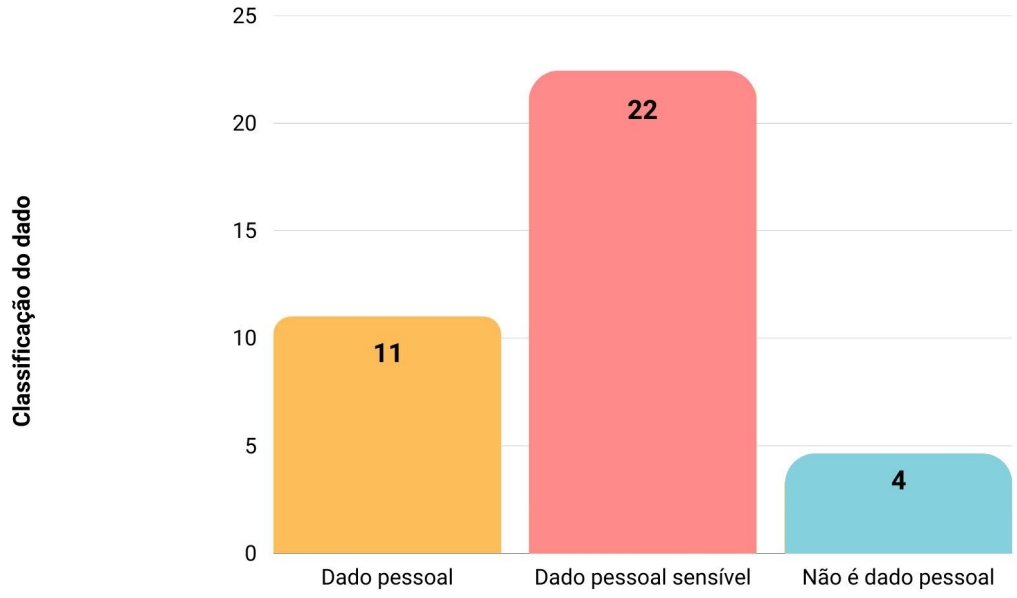

Figura 5 – Classificação dos dados dos pacientes
Fonte: Elaborada pelos autores.

Fizemos a mesma classificação nos dados compartilhados com o MS. A classificação dos dados compartilhados, assim como a definição do fluxo de compartilhamento, é de fundamental importância para a análise dos riscos e deve estar contida no RIPD.

A Figura 6 reflete a proporcionalidade de dados de exames enviados ao MS. Conforme é possível observar, a maior parte dos dados é classificada como pessoal.

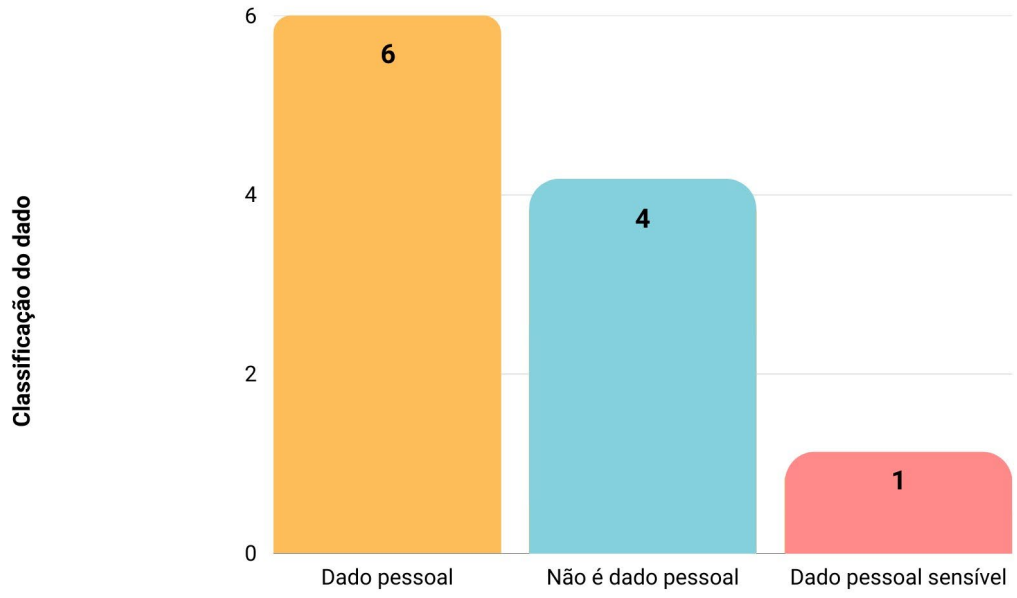

Figura 6 – Classificação dos dados dos exames dos pacientes enviados ao MS
Fonte: Elaborada pelos autores.

Já a Figura 7 reflete a proporcionalidade de dados referente ao envio de indicadores de produção ao MS. Conforme é possível observar, a maior parte dos dados são classificados como pessoais.

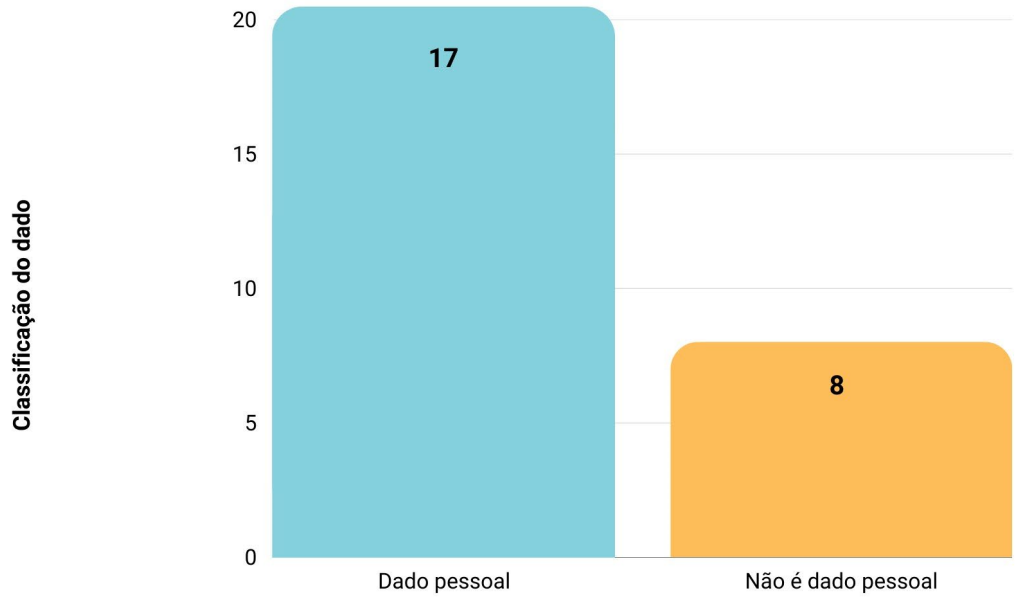

Figura 7 – Classificação dos indicadores enviados ao MS
Fonte: Elaborada pelos autores.

Em síntese, a classificação possibilitou as seguintes conclusões:

1. Dados cadastrais dos profissionais de saúde e gestores – a partir da análise, identificamos que cem por cento dos dados solicitados são classificados como pessoais.
2. Dados dos pacientes – constatamos que a maior parte dos dados solicitados aos pacientes são classificados como sensíveis.
3. Dados dos exames enviados ao MS – a maior parte dos dados é classificada como pessoal.
4. Dados de indicadores de produção enviados ao MS – a maioria dos dados é classificada como não pessoal, ou seja, são dados meramente estatísticos ou anonimizados.
5. Os tratamentos dos dados pessoais e pessoais sensíveis estão legitimados pelos artigos 7º e 11 da LGPD em suas respectivas finalidades.

A última e mais significativa conclusão refere-se à base de legitimidade jurídica do tratamento de dados efetuado pelo Núcleo Telessaúde UFSC. Identificamos as seguintes finalidades:

I) Dados pessoais tratados – as atividades do projeto deixam nítidas, pelo menos, três bases de legitimidade para o tratamento de dados, independentemente de consentimento. São elas: a) tratamento de dados realizado pela administração pública para a execução de políticas públicas, uma vez que o Núcleo Telessaúde UFSC faz parte do Programa Nacional Telessaúde Brasil Redes do MS (inciso III do artigo 7º da LGPD); b) tratamento de dados realizados por órgão de pesquisa, no caso a Universidade Federal de Santa Catarina, que aplica os dados em atividades de pesquisa, cujo escopo é a melhoria da saúde pública (inciso IV do artigo 7º da LGPD); e c) tratamento de dados para a tutela da saúde por profissionais de saúde e serviços de saúde (inciso IX do artigo 7º da LGPD).

II) Dados pessoais sensíveis tratados – mesmo com hipóteses legais mais restritivas, o tratamento de dados pessoais sensíveis realizado pelo Núcleo Telessaúde UFSC encontra, assim como na análise do item anterior, três bases legais, independentemente de consentimento, nos termos do artigo 11 da LGPD. São elas: a) tratamento compartilhado de dados necessários à execução de políticas públicas, pela administração pública (inciso II, alínea "a", do artigo 11 da LGPD); b) tratamento de dados para a realização de estudos, por órgão de pesquisa – no caso, a UFSC (inciso II, alínea "b", do artigo 11 da LGPD); e c) tutela da saúde, em procedimentos realizados por profissionais da área da saúde e/ou autoridades sanitárias (inciso II, alínea "f", do artigo 11 da LGPD).

Após a análise dos itens anteriores foi possível afirmar que o tratamento de dados é realizado de forma proporcional às finalidades informadas, principalmente quando observado o amplo aspecto que envolve o acesso ao direito fundamental à saúde, como referido no artigo 6º da Constituição Federal (BRASIL, 1988).

O Núcleo Telessaúde UFSC realiza o tratamento de dados pessoais e dados pessoais sensíveis com a finalidade de executar políticas públicas de acesso à saúde, desenvolver atividades de pesquisa para a melhoria dos serviços de saúde e corroborar para a tutela da saúde realizada pelos profissionais da área que atuam em diferentes equipes.

Os fluxos demonstram que a adequação e a necessidade são observadas em quase todo o ciclo de tratamento de dados realizado, ou seja, cada dado coletado é tratado de acordo com a finalidade e encontra legitimidade jurídica estabelecida nos artigos 7º e 11 da LGPD.

TERCEIRA E QUARTA ETAPAS: RISCOS AOS DIREITOS DOS TITULARES

Nessas etapas, analisamos o volume de dados, a espécie de dados tratados e os fluxos dos principais ciclos de tratamento e, principalmente, estabelecemos a proteção dos direitos dos titulares de dados e o acesso à saúde como valores/objetivos do Núcleo Telessaúde UFSC. Uma forma de adequação ao princípio da autodeterminação informativa, núcleo axiológico da LGPD.

As análises foram feitas para possibilitar a identificação de eventuais riscos e depois relacioná-los, classificá-los e atribuir-lhes grau de gravidade e de urgência de acordo com os direitos dos titulares potencialmente atingidos.

Importante salientar que a LGPD não conceitua risco, e a melhor doutrina acerca do assunto considera o fato uma qualidade da legislação. A doutrina aponta, ainda, que a análise do risco não se resume a um *checklist* de *compliance*, e que a sua efetivação deve ter como objetivo primário a proteção dos direitos dos titulares de dados (GOMES, 2020).

Evidentemente que, ao falar em direitos dos titulares, não podemos nos limitar aos especificados nos artigos 17, 18, 20, 21 e 22 da LGPD; precisamos levar em consideração os direitos fundamentais e as liberdades civis previstos na Constituição Federal.[4]

A partir da incorporação desses valores/objetivos pode-se utilizar, subsidiariamente, a ABNT NBR ISO 31000:2018, que trata das diretrizes de Gestão de Riscos, e a ABNT NBR ISO/IEC 27002:2013, que trata das Técnicas de Segurança da Informação. Destaca-se que o RIPD não tem por objetivo analisar os riscos para a organização, mas para os direitos dos titulares, e, nesse sentido, as referidas normas são subsidiariamente aplicadas.

4 "Uma das funções do RIPD [Relatório de Impacto à Proteção de Dados Pessoais] é a prevenção e mitigação de riscos aos direitos dos titulares de dados, direitos esses que podemos classificar em três: (i) direitos fundamentais, previstos no art. 5º da Constituição Federal (CF); (ii) liberdades civis ou direitos civis, previstos no artigo 5º da CF; e (iii) direito dos titulares de dados, previstos nos arts. 18, 21 e 22 da LGPD." (Gomes, 2020, p. 271).

Para fins organizacionais, de forma a facilitar as medidas corretivas, os riscos foram classificados em duas grandes categorias, de acordo com a origem de eventuais inconsistências ou inconformidades perante a LGPD e com os consequentes impactos sobre os direitos dos titulares, quais sejam:

I) Riscos organizacionais: decorrentes de falhas ou inconsistências na estrutura organizacional e na gestão do Núcleo Telessaúde UFSC capazes de impactar os direitos dos titulares; e

II) Riscos operacionais: eventual incidente que ocorre durante o processo de tratamento de dados, como falhas no sistema, interrupção das operações, armazenamento inadequado de dados por instituições e por demais atores envolvidos no processo.

Identificados e classificados os riscos, faz-se necessária uma análise acerca dos possíveis impactos aos direitos dos titulares. Essa análise é feita comparando o tratamento de dados descrito nos itens anteriores com o rol de direitos elencados na LGPD e na Constituição Federal.

Foi atribuído, ainda, a cada categoria de risco, um grau de urgência na correção, tendo por base a mesma análise relacional entre direitos e atividades do tratamento de dados, levando em consideração as informações disponibilizadas pelo Núcleo Telessaúde UFSC.

O Quadro 1 apresenta uma síntese da análise dos riscos mapeados no Núcleo Telessaúde UFSC:

Quadro 1 – Resumo da análise de risco

Risco	Direito potencialmente impactado	Grau/urgência	Atividade responsável (organizacional/operacional)
Opacidade sobre o tratamento de dados	Artigo 18, incisos I, II e VII da LGPD	Alto/urgente	Organizacional
Inacessibilidade de informações	Artigo 18, incisos I, II e VII, e artigo 19 da LGPD	Alto/urgente	Organizacional
Inércia perante incidentes de privacidade	Artigo 5°, inciso X, da CF, e artigo 17 da LGPD	Alto/urgente	Organizacional
Incompatibilidade com a conjuntura tecnológica	Artigo 5°, inciso X, da CF, e artigos 17 e 18 da LGPD	Alto/urgente	Organizacional e operacional
Acesso não autorizado	Artigo 5°, inciso X, da CF, e artigos 17 e 18 da LGPD	Alto/não urgente	Organizacional e operacional
Modificação não autorizada	Artigo 5°, inciso X, da CF, e artigos 17 e 18, inciso III, da LGPD	Alto/não urgente	Organizacional e operacional
Perda – Destruição ou extravio de dados pessoais	Artigo 5°, inciso X, da CF, e artigos 17 e 18, incisos II e III, da LGPD	Alto/não urgente	Organizacional e operacional
Apropriação	Artigo 5°, inciso X, da CF, e artigos 17 e 18 da LGPD	Alto/não urgente	Organizacional e operacional
Remoção não autorizada	Artigo 18, incisos II e III, da LGPD	Alto/não urgente	Organizacional e operacional
Coleta excessiva	Decorrente do artigo 6°, inciso III, da LGPD	Baixo/não urgente	Organizacional
Compartilhamento ou distribuição de dados pessoais com terceiros sem o consentimento do titular dos dados pessoais ou sem a informação do compartilhamento	Artigo 5°, inciso X, da CF, e artigos 17 e 18, incisos II e III, da LGPD	Alto/urgente	Organizacional
Retenção prolongada de dados pessoais sem necessidade	Decorrente do artigo 6°, inciso III, e artigo 18, inciso VI, da LGPD	Alto/urgente	Organizacional
Falha ou erro de processamento	Decorrente do artigo 6°, inciso V, da LGPD	Alto/urgente	Operacional
Reidentificação de dados pseudonimizados	Artigo 18, inciso IV, da LGPD	Alto/urgente	Operacional

Fonte: Elaborado pelos autores.

A Figura 8 apresenta a quantidade de riscos desenvolvidos em cada uma das categorias analisadas: organizacional e operacional.

Figura 8 – Quantidade de riscos nas categorias Organizacional e operacional X Organizacional X Operacional
Fonte: Elaborada pelos autores.

Visando a uma melhor visualização do levantamento dos dados e das análises, optou-se por uma ferramenta de gestão comumente utilizada para analisar problemas organizacionais – a matriz GUT (Gravidade, Urgência e Tendência) –, e, a partir dessa análise, buscou-se definir a prioridade para as devidas resoluções.

Por gravidade entende-se o impacto dos riscos analisados em todos os ciclos de tratamento, caso eles venham a acontecer, levando-se em consideração todos os atores, os cenários e as atividades envolvidos. Por urgência entende-se o prazo disponível ou necessário para se sanarem as questões sem ferir os direitos dos titulares dos dados. Quanto maior for a urgência, menor será o tempo disponível para sua resolução. Por tendência entende-se o potencial que esse risco tem de se agravar com o passar do tempo, ou mesmo o potencial de reduzir ou desaparecer.

Assim, analisamos o grau de gravidade e urgência por meio da aplicação da matriz GUT, a fim de mapear a análise e a priorização dos riscos, conforme apresentado na Tabela 1:

Tabela 1 – Matriz GUT da análise dos riscos observados nas atividades organizacionais e operacionais

Risco	Gravidade	Urgência	Tendência	Grau crítico (GxUxT)	Priorização
Opacidade sobre o tratamento de dados	5	5	5	125	1º
Inacessibilidade de informações	5	5	5	125	1º
Inércia perante incidentes de privacidade	5	5	5	125	1º
Incompatibilidade com a conjuntura tecnológica	5	5	5	125	1º
Acesso não autorizado	5	3	3	45	3º
Modificação não autorizada	5	3	3	45	3º
Perda – Destruição ou extravio de dados pessoais	5	2	2	20	4º
Apropriação	5	3	3	45	3º
Remoção não autorizada	5	3	3	45	3º
Coleta excessiva	2	2	2	8	5º
Compartilhamento ou distribuição de dados pessoais com terceiros sem o consentimento do titular dos dados pessoais ou sem a informação do compartilhamento	5	5	5	125	1º
Retenção prolongada de dados pessoais sem necessidade	5	5	4	100	2º
Falha ou erro de processamento	5	5	5	125	1º
Reidentificação de dados pseudonimizados	5	5	4	100	2º

Fonte: Elaborada pelos autores.

Observa-se que na matriz GUT acima, foram inseridos os riscos levantados neste relatório e a partir da multiplicação, foram identificados uma série de riscos em estado máximo de criticidade e com prioridade máxima de que sejam solucionados, por possuir tendência de piorar imediatamente ou a curto prazo.

Independentemente do modelo ou método utilizado (ou adaptado, como nesse caso), o importante é dar centralidade aos direitos dos titulares de dados e fomentar a reflexão por parte dos agentes de tratamento das contínuas e necessárias proteção dos dados pessoais e revisão das práticas realizadas no tratamento.

QUINTA ETAPA: MEDIDAS PARA MITIGAÇÃO DOS RISCOS

Após a análise dos eventuais riscos aos direitos dos titulares de dados, é necessária a adoção de medidas. Assim, elaboramos medidas de acordo com a classificação de riscos, sendo necessária a distribuição de suas implementações para as áreas organizacional e operacional do Núcleo Telessaúde UFSC, bem como o apontamento de um prazo razoável para suas implementações.

O Quadro 2 apresenta os riscos mapeados e as medidas que devem ser tomadas para cada caso. Importante salientar que grande parte delas já foi implementada e que o quadro é meramente exemplificativo.

Quadro 2 – Medidas para os riscos

Risco	Medida a ser adotada	Responsável
Opacidade sobre o tratamento de dados	1 Elaboração da Política de Privacidade do Núcleo Telessaúde UFSC. 2 Capacitação dos colaboradores que atuam no tratamento de dados. 3 Publicação dos fluxos de tratamento de dados, incluindo compartilhamento com órgãos/entidades parceiros.	Área Organizacional do Núcleo Telessaúde UFSC
Inacessibilidade de informações	1 Criação e estruturação de setor (Encarregado de dados). 2 Publicação dos fluxos de tratamento de dados, incluindo compartilhamento com órgãos/entidades parceiros.	Área Organizacional do Núcleo Telessaúde UFSC
Inércia perante incidentes de privacidade	1 Elaboração de um Protocolo de Segurança em caso de incidentes. 2 Capacitação dos colaboradores que atuam no tratamento de dados. 3 Atualização contínua dos Termos de Confidencialidade.	Área Organizacional do Núcleo Telessaúde UFSC
Incompatibilidade com a conjuntura tecnológica	1 Análise e revisão dos sistemas utilizados em relação à conjuntura tecnológica atual. 2 Análise dos sistemas utilizados por operadores e por órgãos/entidades com os quais dados são compartilhados. 3 Política de atualização dos sistemas. 4 Utilizar a NBR ISO/IEC 27002:2013 para as análises. 5 Registro e documentação das referidas atividades.	Área Operacional e Organizacional do Núcleo Telessaúde UFSC
Acesso não autorizado	1 Submeter os sistemas a testes periódicos de vulnerabilidade. 2 Registro e documentação dos testes de vulnerabilidade.	Área Operacional do Núcleo Telessaúde UFSC
Modificação não autorizada	1 Submeter os sistemas a testes periódicos de vulnerabilidade. 2 Registro e documentação dos testes de vulnerabilidade.	Área Operacional do Núcleo Telessaúde UFSC
Perda – Destruição ou extravio de dados pessoais	1 Submeter os sistemas a testes periódicos de vulnerabilidade. 2 Registro e documentação dos testes de vulnerabilidade.	Área Operacional do Núcleo Telessaúde UFSC
Apropriação	1 Submeter os sistemas a testes periódicos de vulnerabilidade. 2 Registro e documentação dos testes de vulnerabilidade.	Área Operacional do Núcleo Telessaúde UFSC
Remoção não autorizada	1 Submeter os sistemas a testes periódicos de vulnerabilidade. 2 Registro e documentação dos testes de vulnerabilidade.	Área Operacional do Núcleo Telessaúde UFSC
Coleta excessiva	Revisão periódica dos dados pessoais e dados pessoais sensíveis a serem coletados, relacionando-os com a finalidade, a adequação e a necessidade do tratamento.	Área Organizacional do Núcleo Telessaúde UFSC
Compartilhamento ou distribuição de dados pessoais com terceiros sem o consentimento do titular dos dados pessoais ou sem a informação do compartilhamento	1 Disponibilizar informações aos titulares de dados acerca do compartilhamento de dados no momento da coleta.	Área Organizacional do Núcleo Telessaúde UFSC
Retenção prolongada de dados pessoais sem necessidade	1 Elaborar e publicizar uma política de armazenamento e eliminação de dados pessoais e dados pessoais sensíveis.	Área Organizacional do Núcleo Telessaúde UFSC
Falha ou erro de processamento	1 Submeter os sistemas a testes de vulnerabilidade. 2 Atualização contínua dos sistemas de acordo com a conjuntura tecnológica atual.	Área Operacional do Núcleo Telessaúde UFSC
Reidentificação de dados pseudonimizados	Revisão dos processos de anonimização e pseudonimização de dados. Ampliação dos referidos processos. Análise da conjuntura tecnológica.	Área Operacional do Núcleo Telessaúde UFSC

Fonte: Elaborado pelos autores.

O RIPD deve sintetizar as medidas a serem adotadas e ser uma base de gestão da informação que permita que os agentes de tratamento executem as medidas de forma eficiente. Tanto os agentes como o encarregado de dados devem revisitar o RIPD para orientar suas ações. O relatório deve ser revisado constantemente em uma periodicidade razoável. Nesse caso, o prazo foi de um ano, pois a conjuntura tecnológica, a mudança de colaboradores, as mudanças regulatórias e outros fatores devem ser incorporados às práticas efetivadas no tratamento de dados.

CONSIDERAÇÕES FINAIS

O artigo teve como objetivo apresentar e discutir as diretrizes para a construção de um RIPD que colabore para a preservação da dimensão humana do dado, considerando a personalidade e a necessidade de preservação de direitos. Por meio de um relato de experiência, o trabalho apresenta e descreve a elaboração do RIPD do Núcleo Telessaúde UFSC, desenvolvido pela equipe de trabalho que também realizou a análise dos riscos decorrentes do tratamento, sempre presente na conjuntura tecnológica atual.

A elaboração do RIPD foi fundamental para constatarmos que, como boa parte da administração pública e das organizações privadas, o Núcleo Telessaúde UFSC efetivou o tratamento de dados de forma incrementalista, pois o seu principal objetivo é a efetivação de uma política pública – no caso, o acesso aos serviços de saúde.

Com a elaboração do referido instrumento, a adoção pontual de boas práticas ou mesmo de atividades de *compliance* é substituída por uma ampla revisão do tratamento e uma reflexão crítica sobre as práticas adotadas pela organização. O foco passa a ser o titular, à medida que as diretrizes da LGPD são aplicadas a cada fase do tratamento. Consequentemente, o núcleo axiológico da norma – qual seja, o princípio da autodeterminação informativa – passa a ser concretizado em práticas corriqueiras, protegendo a dimensão humana do dado.

A principal contribuição do estudo refere-se à elaboração de diretrizes que podem ser seguidas para a elaboração do RIPD e que se mostraram efetivas na aplicabilidade no caso do Núcleo Telessaúde UFSC. Assim, temos um modelo dividido em cinco etapas, centralizado na dimensão humana do dado (direito dos titulares) e executado por uma equipe multidisciplinar capaz de absorver elementos jurídicos, de gestão e de tecnologia da informação. Os itens que devem compor o RIPD, de acordo com a experiência aqui apresentada, são: (1) identificação e definição do organograma, do volume de dados e dos fluxos; (2) classificação dos dados, da finalidade e do propósito de uso; (3) análise dos dados; (4) definição dos riscos aos direitos dos titulares; e (5) definição de medidas para mitigação dos riscos.

Assim, mesmo que a Autoridade Nacional de Proteção de Dados (ANPD) não tenha regulamentado em definitivo as questões que envolvem o RIPD, percebemos a possibilidade de adoção de modelos com metodologias diversas a serem aplicados em diferentes áreas, mas tendo por centralidade a efetivação do princípio da autodeterminação informativa.

Acreditamos que este trabalho apresenta uma importante contribuição por se tratar de um relato de experiência realizado em uma unidade de serviço de saúde, que pode auxiliar outras organizações a se adequarem à nova legislação e à necessidade de construção de um RIPD.

Indicamos que novos estudos ainda são necessários para aprofundar o conhecimento sobre as metodologias utilizadas para mensurar os riscos provenientes do tratamento de dados, sobre os parâmetros para análise da conjuntura tecnológica e sobre a necessária publicização do RIPD.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 fev. 2023.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018, p. 59. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 fev. 2023.

BRASIL. Medida provisória n. 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística [...]. **Diário Oficial da União**, Brasília, DF, 17 abr. 2020a, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 1 fev. 2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade (ADI) 6837**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil (CFOAB). Relatora: Ministra Rosa Weber. Brasília, DF, 24 abr. 2020b. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 1 fev. 2023.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental (ADPF) 722**. Requerente: Rede Sustentabilidade. Relatora: Ministra Cármen Lúcia. Brasília, DF, 20 ago. 2020c. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354. Acesso em: 1 fev. 2023.

DAVENPORT, Thomas H. **Big data at work**: dispelling the myths, uncovering the opportunities. Boston: Harvard Business Review Press, 2014.

FRAZÃO, Ana. Apresentação da obra. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. *E-book*. p. 5-22.

GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In*: PALHARES, Felipe (coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020. p. 245-271.

GOMES, Maria Cecilia Oliveira. LGPD: desafios da regulamentação do relatório de impacto. **Jota**, São Paulo, 11 fev. 2021. Accountability. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. Acesso em: 1 fev. 2023.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. São Paulo: Companhia das Letras, 2016.

KELLOGG, Katherine; VALENTINE, Melissa; CHRISTIN, Angèle. Algorithms at work: the new contested terrain of control. **Academy of Management Annals**, Reino Unido, v. 14, n. 1, p. 366-410, 2020. Disponível em: https://angelechristin.com/wp-content/uploads/2020/01/Algorithms-at-Work_Annals.pdf. DOI: https://doi.org/10.5465/annals.2018.0174. Acesso em: 10 maio 2023.

LEONARDI, Paul M.; TREEM, Jeffrey W. Behavioral visibility: a new paradigm for organization studies in the age of digitization, digitalization, and datafication. **Organization Studies**, Reino Unido, v. 41, n. 12, p. 1601-1625, 2020. Disponível em: https://journals.sagepub.com/doi/10.1177/0170840620970728. DOI: https://doi.org/10.1177/0170840620970728. Acesso em: 10 maio 2023.

MATTAR, Fauze Najib. **Pesquisa de marketing**. São Paulo: Atlas, 2001. v. 3.

MENDES, Laura Schertel F. Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1-18, 2020. DOI: https://doi.org/10.5020/2317-2150.2020.10828. Disponível em: https://periodicos.unifor.br/rpen/article/view/10828/pdf. Acesso em: 10 maio 2023.

MINAYO, Maria Cecília de Souza (org.). **Pesquisa social**: teoria, método e criatividade. Petrópolis: Vozes, 2001.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação: Maria Celina Bodin Moraes; Tradução: Danilo Doneda e Laura Doneda. Rio de Janeiro: Renovar, 2008.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. London: Profile Books, 2019.