UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO - UNIDADE SANTA RITA
COORDENAÇÃO DE MONOGRAFIAS

MARIA BEATRIZ VICENTE

O CASO KLARA CASTANHO E A PROTEÇÃO DE DADOS NA SAÚDE SUPLEMENTAR: UMA ANÁLISE CRÍTICA SOB A LUZ DO ORDENAMENTO JURÍDICO E REGULATÓRIO BRASILEIRO E DO *COMPLIANCE* COMO FERRAMENTA DE PRIVACIDADE

SANTA RITA - PB
2025

MARIA BEATRIZ VICENTE

O CASO KLARA CASTANHO E A PROTEÇÃO DE DADOS NA SAÚDE SUPLEMENTAR: UMA ANÁLISE CRÍTICA SOB A LUZ DO ORDENAMENTO JURÍDICO E REGULATÓRIO BRASILEIRO E DO *COMPLIANCE* COMO FERRAMENTA DE PRIVACIDADE

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Unidade Santa Rita, do Centro de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial para a obtenção do título de Bacharela em Ciências Jurídicas.

Orientador: Dr. Adriano Marteleto Godinho

SANTA RITA - PB
2025

Catalogação na publicação
Seção de Catalogação e Classificação

V632c Vicente, Maria Beatriz.
O caso Klara Castanho e a proteção de dados na saúde suplementar: uma análise crítica sob a luz do ordenamento jurídico e regulatório brasileiro e do compliance como ferramenta de privacidade / Maria Beatriz Vicente. - João Pessoa, 2025.
57 f. : il.

Orientação: Adriano Marteleto Godinho.
TCC (Graduação) - UFPB/DCJ.

1. Compliance. 2. Direito fundamental. 3. Proteção de dados. I. Godinho, Adriano Marteleto. II. Título.

UFPB/DCJ/CCJ-SANTARITA CDU 34

Elaborado por Amanda Souza Xavier de Luna - CRB-15/817

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
DIREÇÃO DO CENTRO
COORDENAÇÃO DE MONOGRAFIAS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
DISCIPLINA: TRABALHO DE CONCLUSÃO DE CURSO

CCJ Centro de Ciências Jurídicas

ATA DE DEFESA PÚBLICA DE TRABALHO DE CONCLUSÃO DE CURSO

Ao décimo dia do mês de Abril do ano de dois mil e vinte e cinco, realizou-se a sessão de Defesa Pública do Trabalho de Conclusão do Curso de Direito intitulado "O caso Klara Castanho e a proteção de dados na saúde suplementar: uma análise crítica sob a luz do ordenamento jurídico e regulatório brasileiro e do compliance como ferramenta de privacidade", do(a) discente(a) **MARIA BEATRIZ ViCENTE**, sob orientação do(a) professor(a) Dr. Adriano Marteleto Godinho. Após apresentação oral pelo(a) discente e a arguição dos membros avaliadores, a Banca Examinadora se reuniu reservadamente e decidiu emitir parecer favorável à APROVAÇÃO, de acordo com o art. 33, da Resolução CCGD/02/2013, com base na média final de 10,0 (dez). Após aprovada por todos os presentes, esta ata segue assinada pelos membros da Banca Examinadora.

Dr. Adriano Marteleto Godinho

Me. Alex Taveira dos Santos

Dra. Ana Carolina Couto Matheus

AGRADECIMENTOS

Agradeço à minha mãe, Rosimeri, meu símbolo de perseverança e força, que com toda sua personalidade me ensinou que o caminho para o sucesso é tentar até o alcançar, não se abalando por qualquer falha. À minha segunda mãe, Silvana, que me apoiou em todos os momentos difíceis da vida e me ensinou a ser a mulher profissional e dedicada que sou hoje.

Ao meu namorado, José Neto, o qual através do seu amor calmo e gentil, me amparou durante parte dessa graduação, sempre acreditando que sou melhor do que acredito.

Às minhas amigas da vida, minhas almas gêmeas, o meu grupo de ensino médio: *Painkillers*. Brena e Laís foram e são um alicerce bem definido na minha vida, estando sempre presentes para apoiar ou criticar, sempre agindo para contribuir com o meu crescimento.

Ao meu grupo da faculdade, que me acolheu com tanta felicidade, se fazendo presente. Sem vocês, estes cinco anos e todas as suas dificuldades seriam mais pesados para aguentar.

Agradeço aos meus amigos e colegas do setor de Governança, Compliance, Riscos e Proteção de Dados da Unimed João Pessoa. Sem eles não saberia metade do conhecimento necessário para a produção desse trabalho, não seria metade da profissional que sou e não teria dado tanta risada trabalhando de segunda a sábado durante a graduação. Em especial, agradeço ao meu grande amigo e mentor, Victor Patriota, o qual me recebeu, me orientou e me permitiu crescer, sempre atuando para me ver ascender no trabalho.

Agradeço ao meu orientador, Prof. Dr. Adriano Godinho. O qual por meio da sua didática impecável despertou a minha paixão pelo direito e pelo direito civil, tornando as aulas noturnas um momento à se esperar durante o período letivo. Além disso, com sua paciência e gentileza, orientou-me até nas regras de uso de crase, indo além da breve orientação do trabalho.

Por fim, agradeço à minha equipe do 2º Juizado Especial da Fazenda Pública da Capital, os quais me acolheram, instruíram e nutriram minha paixão por fazer o direito de todos ser apreciado com toda a competência possível. Agradeço à assessoria do gabinete, na forma de Ronald Bottecchia, aos leigos que destinavam um tempo do seu trabalho para sempre debaterem e tirarem minhas dúvidas e à Vossa Excelência, Erica Tatiana Amaral Soares Freitas, que em um ano e meio transformou a minha visão do judiciário e a profissional que sou.

A injustiça em qualquer lugar é uma ameaça à justiça por toda parte. - Martin Luther King

RESUMO

O presente trabalho propôs um estudo sobre como o *compliance* pode ser empregado como ferramenta estratégica para prevenir vazamentos de dados no âmbito da saúde suplementar, tomando como estudo de caso, o vazamento da atriz Klara Castanho. Para isso, analisou o marco regulatório brasileiro de proteção de dados e as normas do setor de saúde suplementar, com enfoque na Lei Geral de Proteção de Dados (LGPD), nas Resoluções Normativas da Agência Nacional de Saúde Suplementar (ANS) e na legislação correlata. A metodologia adotada consistiu na pesquisa bibliográfica, documental e jurisprudencial. Assim, os resultados demonstraram que a implementação de programas de compliance estruturados - contemplando mapeamento de fluxos de dados (Data Mapping), elaboração de Relatórios de Impacto à Proteção de Dados (RIPD), capacitação continuada de colaboradores, constitui mecanismo um essencial para conformidade regulatória. Logo, o caso analisado evidenciou ainda a necessidade de articulação entre as esferas administrativa (ANPD e ANS), civil e ético-profissional (Conselhos de Classe) para efetiva responsabilização dos envolvidos em casos similares e a garantia da justiça para a vítima. E, quando analisado o caso concreto da atriz, a atuação dos poderes foi ineficaz, deixando de aplicar sanções cabíveis e garantir a proteção dos direitos fundamentais de Klara.

Palavras-chave: *Compliance*. Proteção de dados. Direitos fundamentais. Saúde suplementar.

ABSTRACT

This paper proposed a study on how compliance can be used as a strategic tool to prevent data breaches in the supplementary health sector, using the data leak involving actress Klara Castanho as a case study. To this end, it analyzed the Brazilian regulatory framework for data protection and the regulations specific to the supplementary health sector, with a focus on the General Data Protection Law (LGPD), the Normative Resolutions of the National Supplementary Health Agency (ANS), and related legislation. The methodology adopted included bibliographic, documentary, and jurisprudential research. The results showed that the implementation of structured compliance programs — including data flow mapping, the preparation of Data Protection Impact Reports (DPIA), and ongoing employee training — constitutes an essential mechanism for regulatory compliance. The case under analysis also highlighted the need for coordination between administrative (ANPD and ANS), civil, and ethical-professional (Professional Councils) spheres to ensure accountability for those involved in similar incidents and to guarantee justice for the victim. However, when examining the specific case of the actress, the actions of the authorities showed to be ineffective, failing to impose appropriate sanctions and to protect Klara's fundamental rights.

Keywords: *Compliance*. Data protection. Fundamental rights. Supplementary health.

SUMÁRIO

1 INTRODUÇÃO 10

2 O DESENVOLVIMENTO DO DIREITO A PROTEÇÃO DOS DADOS PESSOAIS NA EUROPA E NO ORDENAMENTO JURÍDICO BRASILEIRO 12

2.1 Legislações Regulamentadoras do Direito à Proteção de Dados 14

2.1.1 Constituição Federal de 1988 e a Emenda Constitucional n.º 115 15

2.1.2 A Perspectiva da Privacidade no Código Civil Brasileiro 16

2.1.4 Lei n.º 12.965, de 23 de abril de 2014 – Lei do Marco Civil da Internet 17

2.1.4 Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados 18

3 NORMAS E LEGISLAÇÕES REGULAMENTADORAS DA PROTEÇÃO DE DADOS NA SAÚDE SUPLEMENTAR 23

3.1 Normas dos Conselhos de Classe: Conselho Federal de Medicina e do Conselho Federal de Enfermagem 23

3.2 Resolução Normativa n.º 507, de 30 de março de 2022, da Agência Nacional de Saúde Suplementar 25

3.3 Resolução Normativa n.º 518, de 29 de abril de 2022, da Agência Nacional de Saúde Suplementar 26

3.4 Lei n.º 12.846, de 1º de agosto de 2013 – Lei Anticorrupção 27

3.5 *Compliance* Empresarial 28

3.5.1 *Compliance* Digital 30

3.6 Programa de Integridade 32

4 O CASO KLARA CASTANHO E O VAZAMENTO DE DADOS NO ÂMBITO DA SAÚDE SUPLEMENTAR 37

4.1 Análise do Caso Sob a Luz da Legislação Brasileira na Perspecitiva Judicial 40

4.2 Análise do Caso Sob a Luz da Legislação Brasileira na Perspectiva Regulatória 45

5 CONSIDERAÇÕES FINAIS 50

1 INTRODUÇÃO

O presente trabalho irá abordar a temática acerca do caso da atriz brasileira Klara Castanho e proteção de dados na saúde suplementar, com o desafio do sigilo e a utilização do *compliance* como ferramenta de privacidade, propondo um estudo entre as normativas que regulamentam a proteção de dados no Brasil, dentro e fora do âmbito da saúde suplementar, as normas violadas no caso e implicação de tais violações à atriz.

Em 2022, a mídia brasileira divulgou que a atriz Klara Castanho teria entregado seu filho para a adoção, sem demais detalhes, ainda enquanto a atriz estava no hospital se recuperando do parto. *A priori*, ditou a imprensa que a informação havia sido obtida por meio de uma enfermeira do Hospital e Maternidade Brasil, administrado pela Rede D'OR São Luiz, a qual, obteve acesso ao prontuário da atriz e, assim, divulgou o ocorrido.

Após o fato, a atriz veio a público informar que o referido ato de entrega à adoção havia ocorrido de forma voluntária, tendo em vista a natureza da concepção do bebê, o qual havia sido gerado após uma violência sexual. Ademais, ressaltou que tais informações eram sigilosas e não deveriam ter sido divulgadas ao público sem o seu consentimento.

Nesse sentido, quando em análise ao caso, torna-se evidente que a proteção de dados dos titulares no âmbito hospitalar é desafiadora, uma vez que além depender da ética profissional de cada indivíduo e da compreensão da importância da proteção ao sigilo do paciente, também depende da devida atuação das operadoras de saúde suplementar, ao trabalhar para evitar e combater quaisquer formas de vazamentos.

Na atualidade, com o avanço das ferramentas digitais e o acesso a estas, o compartilhamento de informações ocorre de forma desenfreada e facilitada para todos. Tornando-se essencial o estabelecimento de barreiras para impedir que qualquer informação seja disseminada sem o consentimento do titular, violando seu direito à privacidade e infringindo as regras de ética do profissional.

Logo, a problemática reside em torno da questão: como o *compliance* pode ser utilizado para combater a disseminação e vazamento de informações de pacientes/titulares no âmbito da saúde suplementar, evitando a perpetuação de casos como o da atriz Klara Castanho.

Nesse sentido, para o desenvolvimento do trabalho haverá a exploração das legislações e normativas brasileiras acerca da temática, abordando o que pode ser realizado pelas empresas operadoras de saúde suplementar, como meio de prevenção, assim como quais sanções podem ser aplicadas como forma de penalidade e contenção para evitar futuros casos.

Assim, objetivo principal do trabalho consiste em estudar as legislações e normativas brasileiras sobre proteção de dados na saúde suplementar, traçando um paralelo entre o caso Klara Castanho e definindo como a implementação do *compliance* na saúde suplementar pode auxiliar na minimização dos riscos de vazamento de dados.

Para isso, o método de abordagem será o descritivo bibliográfico, beneficiando-se dos instrumentos de pesquisa por meio da documentação direta (pesquisa bibliográfica em livros, artigos, revistas, dissertações, etc) e documental (documentos eletrônicos, leis, decisões administrativas e judiciais).

Além disso, haverá a exploração do problema baseado nos fatos divulgados pela mídia brasileira acerca do caso Klara Castanho, estudando o caso, suas implicações e formas de combate.

Assim, o trabalho se desenvolverá de modo a compreender, no primeiro capítulo, o desenvolvimento dos dados pessoais sob o ordenamento jurídico, entendendo sua importância - tanto por questões de privacidade, quanto por proteção do seu uso como meio de obtenção de vantagens econômicas ilícitas - e quais medidas legislativas foram desenvolvidas para abarcar a questão.

No segundo capítulo, quais normas foram desenvolvidas no âmbito do nicho da saúde suplementar pelo seu órgão regulador, para acompanhar as legislações brasileiras e, assim, quais medidas as operadoras de saúde, por meio de sua equipe de *compliance*, podem utilizar para adequar suas empresas, de modo a evitar e conter situações, quanto ao tratamento e vazamento de dados.

Com isso, no terceiro capítulo, será possível compreender e aprofundar-se na extensão do caso Klara Castanho, de modo a estudá-lo sob tal ótica e em paralelo aos entendimentos dos tribunais do país em tais casos. Para, por fim, chegar a uma conclusão quanto o tema em estudo.

2 O DESENVOLVIMENTO DO DIREITO A PROTEÇÃO DOS DADOS PESSOAIS NA EUROPA E NO ORDENAMENTO JURÍDICO BRASILEIRO

Em 2022, ano de ocorrência do caso a ser explorado neste trabalho, de acordo com dados da *Check Point* (2022), os golpes virtuais na saúde aumentaram em 60% em relação a 2021, determinando que o segmento fica em segundo lugar do ranking, ficando atrás apenas da área de varejo.

Atualmente, no relatório mais recente do *Check Point Research* (2025), publicado em 2025, mas relativo ao ano de 2024, a área da saúde segue em segundo lugar como alvo de invasões e tentativas de golpes virtuais, ainda ficando atrás da área de varejo. Em geral, a área da saúde se torna tão atrativa pela particularidade da delicadeza de suas operações, de modo que, um ataque cibernético ou um vazamento por erro interno ocasiona impactos (econômicos e reputacionais) para a organização, tendo em vista a grande quantidade de dados que estas empresas coletam e como os utilizam para o tratamento de pacientes.

Segundo a Agência Senado (2024), 24% dos brasileiros acima de 16 anos foram vítimas de golpes digitais entre 2023 e 2024, sendo mais 40,85 milhões de pessoas que sofreram prejuízo econômico em decorrência de algum crime cibernético como clonagem de cartão, fraudes ou invasão de contas bancárias. Torna-se evidente como a privacidade e a proteção aos dados tem tornado-se cada vez mais frágil, uma vez que seu valor é imenso em face das inúmeras possibilidades de uso de dados coletados. Contudo, ainda que se quantifique os dados vazados e ataques cibernéticos realizados em determinada área, o vazamento de dados por troca de informações por funcionários das empresas é quase impossível de se quantificar e rastrear. Ou seja, a maior falha e ponto de importância de uma organização resta na mão de obra empregada, a qual deve estar ciente da natureza da sua atividade e das consequências legais e morais, tanto para o paciente, quanto para a organização e para o profissional responsável.

Internacionalmente, a realidade de combate ao vazamento de dados é bem diferente do Brasil, onde há legislações bem definidas e disseminadas com sanções drásticas às empresas, a fim de trazer além do caráter educativo o caráter punitivo a quem não está adequado. O caráter educativo diz respeito à intenção de aplicar medidas sancionatórias com a intenção de chamar a atenção para um problema, como o exemplo da aplicação de uma leve multa por deixar de forma omissa um termo de consentimento de tratamento de dados. Enquanto o caráter punitivo diz respeito a aplicação de sanções com o fim de atuar de forma rigorosa, impondo medidas que irão impactar no andamento da empresa, como, por exemplo, a suspensão de suas atividades pelo descumprimento da lei, ou ainda, a imposição de multa ao faturamento bruto da empresa.

O continente europeu, por meio da União Europeia, ficou conhecido pelo pioneirismo e desenvolvimento de normativas de referência na área de proteção de dados pessoais. O surgimento das legislações está diretamente relacionado com a evolução dos modelos de negócios, os quais passaram a produzir grandes fluxos de dados e por conseguinte, depender fortemente de bases dados, tanto dentro do continente, quanto com o mundo inteiro.

Dessa forma, em 2016, o Parlamento Europeu e o Conselho da União Europeia promulgaram o Regulamento n.º 679 (UNIÃO EUROPEIA) quanto à proteção dos direitos naturais da pessoa no tratamento e compartilhamento de dados. A normativa buscou a proteção dos titulares no tratamento de dados, por entenderem como um direito fundamental previsto na Carta de Direitos Fundamentais da União Europeia e no Tratado de Funcionamento da União Europeia. Como objetivo principal, a legislação estabeleceu princípios e regras de proteção de dados, no âmbito da União Europeia, independentemente da nacionalidade ou residência do titular, tendo ainda como intenção a garantia da liberdade, segurança e justiça de uma união econômica, progresso social, fortalecimento e agrupamento de economias dentro do mercado interno e o bem-estar dos indivíduos.

Após sua promulgação a normativa passou por diversas emendas, como a Diretiva n.º 680 (UNIÃO EUROPEIA) e a Regulamentação n.º 1.725 de 2018 (UNIÃO EUROPEIA), até ser publicado o documento final da matéria: o Regulamento Geral de Proteção de Dados - RGPD, de 2018 (UNIÃO EUROPEIA). O RGPD instituiu de forma mais assertiva e convicta as normativas gerais de proteção de dados, estabelecendo: a proteção de dados no tratamento pelo setor público e privado, o tratamento de dados diferenciado quando utilizado para fins de investigação pelos órgãos de polícia e o controle e acesso dos titulares no tratamento de seus dados.

Com a consolidação do RGPD, o mercado internacional reagiu rapidamente para adequar-se aos itens da legislação europeia e, ainda, alterar suas normativas internas para assim, mudar seus modelos de negócios, tudo isto para evitar que suas economias fossem prejudicadas, uma vez que qualquer empresa inadequada estaria fora da lista de relações comerciais e enfrentaria uma barreira econômica de grande impacto.

No contexto brasileiro, antes do desenvolvimento de legislações específicas para a proteção dos dados pessoais, a privacidade já era um direito fundamental do ser humano, com previsão na Constituição Federal de 1988, sob a forma do art. 5º, inc. X, no qual dita que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...].”(BRASIL). Isto é, ainda que houvesse este vácuo no ordenamento jurídico entre a promulgação da Carta Magna

e a legislação de proteção de dados, havia uma previsão quanto a proteção ao direito básico da privacidade, como meio de combate à disseminação de informações pessoais.

Contudo, apenas em 2018, com a disseminação do GDPR, foi sancionada no Brasil a legislação pertinente a proteção de dados dos titulares: a Lei n.º 13.709 de 14 de agosto de 2018, denominada de Lei Geral de Proteção de Dados, a qual dispõe no *caput* do seu art. 1º, que a legislação possui como objetivo o:

> tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL)

Em seu art. 5º, incisos I e II, a legislação estabelece as definições para dados pessoais e dados pessoais sensíveis. Assim, são dados pessoais toda "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018), e são dados pessoais sensíveis todo "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018).

Com a definição, possibilita-se visualizar a correlação entre os perigos e índices de golpes apontados com a natureza personalíssima dos casos, ou seja, compreende-se como os dados pessoais tratam não apenas de um nome ou de um endereço de e-mail, mas sim de um conjunto de informações que se direcionam a cada indivíduo, tendo então, a visão de como cada vazamento, golpe ou fraude é efetuado de forma direcionada e específica à cada indivíduo.

Dessa forma, a promulgação da lei tornou palpável, quantificável e passível de proteção tais informações. Ainda que houvesse a proteção à privacidade como direito fundamental, o tema era abordado de forma difusa e sem objetividade. Com a GDPR e com a criação da LGPD, possibilitou-se a definição de padrões específicos de segurança, de modo a permitir auferir de forma auditável se o compromisso com a proteção de dados está sendo cumprido, por meio da análise de indicadores e de documentos específicos para uma melhor governança dos dados pessoais, conforme compreende Peck (2021).

2.1 Legislações Regulamentadoras do Direito à Proteção de Dados

Ainda que a Constituição Federal de 1988 previsse o direito à privacidade como um direito fundamental a todos e o Código Civil Brasileiro de 2002 previsse a proteção aos direitos de personalidade, restava a lacuna no ordenamento jurídico para a proteção dos dados pessoais, tanto no âmbito da internet, quanto no âmbito da realidade fora das redes.

Assim, tendo em vista o avanço das normativas internacionais, especialmente na União Europeia, o país passou a desenvolver normativas para preencher tais lacunas como a Lei n.º 12.965 de 2014, conhecida como o Marco Civil da Internet, a qual traz princípios, garantias, direitos e deveres para o uso da Internet no Brasil, regulamentando de forma geral o uso da rede pelos usuários do país, e a Lei n.º 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados, a qual disciplina a coleta, tratamento, compartilhamento - nacional e internacional - e descarte de dados no país, pelos setores públicos e privados.

2.1.1 Constituição Federal de 1988 e a Emenda Constitucional n.º 115

Pedro Lenza, dita que "no direito percebe-se um verdadeiro escalonamento de normas, uma constituindo validade de outra, numa verticalidade hierárquica" (2016, p. 85). Tal percepção deriva da Teoria Pura do Direito, de Hans Kelsen (2000), na qual, as normas são feitas e vistas sob a ótica de uma pirâmide invertida. Aplicando a teoria ao ordenamento jurídico brasileiro, vemos que a Constituição Federal ocupa a posição inicial na pirâmide, servindo de parâmetro para a criação de demais normativas, de modo que estas devem nunca ir de encontro com a norma superior e devem ser desenvolvidas para preencher as lacunas deixadas por esta.

Dessa forma, quanto ao tema em análise, a Constituição Federal Brasileira de 1988, inicialmente, previu a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, como um direito fundamental, sob a forma do art. 5º, X. Todavia, tal previsão englobava direitos individuais específicos, mas ainda de forma difusa, sem uma devida especificação quanto aos dados pessoais (BRASIL).

Apenas em 2022, quatro anos após a LGPD, foi promulgada a Emenda Constitucional n.º 115 (EC n.º 115), e posteriormente transformada no art. 5º, LXXIX, o qual prevê a garantia do direito fundamental de proteção aos dados pessoais, inclusive (mas não taxativamente) nos meios digitais.

Para uma melhor compreensão, é importante diferenciar os direitos previstos no art. 5º, X daquele previsto sob o art. 5º, LXXIX, ambos da Constituição. Assim, os direitos do art. 5º, X, à intimidade, a vida privada, a honra e a imagem das pessoas, sob a perspectiva do ordenamento jurídico brasileiro, diz muito a respeito de aspectos como o sigilo bancário, a proibição da revista íntima a funcionárias e clientes do sexo feminino em empresas privadas e órgãos públicos. Por outro lado, o direito previsto na forma do art. 5º, LXXIX, diz respeito ao direito à proteção de dados pessoais, inclusive nos meios digitais, ou seja, à garantia da coleta, tratamento e compartilhamento adequado, conforme a legislação aplicável e os princípios norteadores desta (BRASIL).

2.1.2 A Perspectiva da Privacidade no Código Civil Brasileiro

Retornando ao modelo de compreensão das normas em pirâmide, de Kelsen (2000), o Código Civil Brasileiro encontrara-se logo abaixo da Constituição Federal. Assim, deve o estudo dos direitos aplicados ao caso serem estudados conforme a mesma perspectiva.

Isto posto, o direito à proteção da intimidade, à vida privada, à honra e à imagem das pessoas, previsto constitucionalmente, também pode ser visto de forma similar no Código Civil, sob a tutela dos direitos de personalidade.

Para Farias e Rosenvald, direitos de personalidade, são:

> [...] aqueles direitos subjetivos reconhecidos à pessoa, tomada em si mesma e em suas necessárias projeções sociais. Enfim, são direitos essenciais ao desenvolvimento da pessoa humana, em que se convertem as projeções físicas, psíquicas e intelectuais do seu titular, individualizando-o de modo a lhe emprestar segura e avançada tutela jurídica. (2006, p. 101 e 102)

Já para Venosa, são:

> Os direitos da personalidade são os que resguardam a dignidade humana. Desse modo, ninguém pode, por ato voluntário, dispor de sua privacidade, renunciar à liberdade, ceder seu nome de registro para utilização por outrem, renunciar ao direito de pedir alimentos no campo de família, por exemplo. Tais direitos buscam a proteção dos atributos da personalidade que determinam a individualidade de todos, os quais os tornam identificáveis e únicos. (2023, p. 306)

Dessa forma, diante da natureza de tais direitos, o ordenamento jurídico dispôs de normas específicas para a garantia do seu resguardo.

Nesse sentido, em referência ao caso em estudo, é possível citar o art. 17 do Código Civil de 2002 o qual dita que “o nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.” (BRASIL). Em adição, o art. 21 do Código Civil de 2002, também dita que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.” (BRASIL).

Contudo, tal previsão não é vista ou considerada para a mídia brasileira, principalmente, no caso da atriz Klara Castanho. A divulgação do ato de entrega do seu filho para a adoção gerou comoção no país, uma vez que a notícia divulgada sequer citava as motivações da atriz, deixando ao público para supor que o ato tinha sido motivado por uma simples vontade de não prosseguir com a criação do bebê - ato indesculpável para a sociedade antiquada e machista do país.

Com a divulgação de sua vida privada houve o dano, e uma vez havendo o dano, o Código Civil prevê o dever de reparação, mediante a imputação da responsabilidade civil.

De acordo com Venosa:

> O termo responsabilidade é utilizado em qualquer situação na qual alguma pessoa, natural ou jurídica, deva arcar com as consequências e um ato, fato ou negócio danoso. Sob essa noção, toda atividade humana, portanto, pode acarretar o dever de indenizar. (2023, p.748)

Em sentido amplo, a responsabilidade diz respeito à atribuição a um sujeito o dever se assumir as consequências de um ato que o tenha realizado. Contudo, para fins de imputação da responsabilidade é necessário considerar a conduta do agente, se o ato decorreu de forma dolosa, omissa ou superveniente a sua vontade, isto é, se houve culpa do agente causador do dano.

Na visão de Tartuce, inexiste um posicionamento doutrinário unânime quanto aos elementos estruturais da responsabilidade civil ou os pressupostos do dever de indenizar, tendo apenas como único item em comum a verificação da culpa do agente. Para o autor, são apontados quatro pressupostos do dever de indenizar: a conduta humana, culpa genérica, nexo de causalidade, dano ou prejuízo (2023).

A conduta humana pode ser causada por uma ação ou pela falta dela, mediante a omissão. Já a culpa deriva do dolo ou da culpa estrita, sendo o dolo uma ‘violação intencional do dever jurídico de prejudicar outrem” (TARTUCE, 2023, p. 1097) e a culpa estrita decorrente de uma ação ou omissão, na qual o agente não possui a intenção do efeito. Para além, o nexo de causalidade deve ser interpretado como uma relação de causa e efeito, isto é, o ato provocado pelo agente contribuí integralmente para o efeito danoso gerado a outrem. Assim, o dano ou prejuízo será a comprovação do dano patrimonial ou extrapatrimonial suportado por alguém (TARTUCE, 2023, p. 1135).

Logo, em que pese a capacidade de interpretação extensiva de todos os instrumentos jurídicos e fundamentais do direito civil para a análise do caso, faz-se necessário a restrição do estudo aos direitos fundamentais, de personalidade e a responsabilidade civil imputada para a reparação dos danos causado a estes.

2.1.4 Lei n.º 12.965, de 23 de abril de 2014 – Lei do Marco Civil da Internet

Seguindo a ordem da pirâmide de Kelsen (2000), adentra-se ao estudo das legislações brasileiras de proteção de dados. A Lei n.º 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. A legislação foi a primeira normativa brasileira, a prever de forma específica a proteção de dados pessoais, ainda que apenas no âmbito do uso da internet.

Dessa forma, a lei inovou ao disciplinar os critérios para uso da internet e os limites dos usuários, de modo que enquanto garantia direitos constitucionais fundamentais, como: a liberdade de expressão, comunicação e manifestação de pensamento, mas também vedou quaisquer atos contra a privacidade, dados pessoais e de segurança da rede e de suas informações.

Contudo, é importante salientar que o Marco Civil da Internet não possui um caráter sancionatório ou regulador do público geral, servindo apenas de diretriz e orientação. Quando em análise das sanções previstas, verifica-se apenas a previsão para sanções econômicas ou administrativas - como advertências, multas e suspensão de atividades - para empresas, ou seja, não há que se falar em responsabilização de indivíduos pelas infrações cometidas, nem em que se falar em medidas incisivas para empresas que atuam de modo a infringir a lei.

Logo, é possível visualizar como tal cenário levou à necessidade da redação e promulgação de uma normativa que abarcasse tais pontos, tendo em vista tal lacuna no ordenamento jurídico brasileiro.

2.1.4 Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados

Igualizada no patamar da pirâmide kelseniana, a Lei n.º 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi promulgada pelo então presidente Michel Temer, em 14 de agosto de 2018, sendo originária do Projeto de Lei Complementar n.º 53 de 2018.

Inicialmente, o prazo estabelecido para a adaptação à lei foi de dezoito meses, posteriormente, o prazo foi prorrogado por mais seis meses e com o contexto pandêmico da sua publicação, tal prazo foi prorrogado novamente. Ficando então estabelecido pela Lei n.º 14.010 de 2020 que apenas a partir do dia 1º de agosto de 2021 iniciar-se-ia a aplicação das sanções previstas na legislação, isto é, a lei passaria a surtir efeitos nas organizações que a descumprissem.

A LGPD, dita em seu art. 1º, acerca da sua finalidade:

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)

Conforme o entendimento de Patrícia Peck acerca da criação da lei:

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da

> informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis. (2021, p.21)

Dessa forma, ainda que a lei tenha sido criar para acompanhar o mercado internacional e evitar o desequilíbrio econômico, é possível reconhecer que também houve a iniciativa de garantia dos direitos dos titulares, tendo em vista que sua redação acompanha princípios intrínsecos ao ordenamento jurídico brasileiro, os quais já estão bem perpetuados.

Todavia, traçando um comparativo com o RGPD, a LGPD é significativamente menor, contendo 10 capítulos e aproximadamente 60 artigos - levando em consideração a quantidade de artigos vetados desde 2018 -, enquanto a normativa europeia possui 11 capítulos e 99 artigos. Assim, é possível aferir e indagar-se quanto a quais lacunas a normativa brasileira possui. Por exemplo, sendo menor e mais subjetiva a normativa criou alguns pontos de insegurança jurídica, tal como os prazos, no qual, onde RGPD prevê um prazo de 72 horas, a LGPD prevê "um prazo razoável", isto é, abre-se a lei para a interpretação extensa dos interessados, seja para a empresa um prazo razoável de um ano, seja para o titular o prazo razoável de uma hora, ou seja, para a autoridade fiscalizadora o prazo razoável de seis meses, cabendo então, ao judiciário a missão de "legislar" e introduzir um prazo considerado razoável.

Passando ao estudo da LGPD, é importante salientar as definições trazidas pela normativa. São elas previstas na forma do art. 5º e seus incisos, e ditam que:

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
>
> IX - agentes de tratamento: o controlador e o operador;
>
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
>
> [...]

> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (BRASIL, 2018)

Faz-se importante mencionar que a lei se aplica a todos os que realizam o tratamento de dados pessoais, sejam organizações públicas ou privadas, pessoas físicas ou jurídicas, desde que tal tratamento ocorra em território nacional, tenha por objetivo a oferta ou fornecimento de bens ou serviços, ou tratamento de dados localizados no território nacional, ou que tenham sido coletados também. Entretanto, em caráter de exceção, a lei não se aplica quando o tratamento é realizado por uma pessoa física, exclusivamente para fins particulares e não econômicos, jornalísticos, artísticos e para fins de segurança pública e defesa nacional, conforme prevê o art. 4º, I, II, III e IV (BRASIL, 2018).

Diferentemente de outras leis nacionais, a LGPD é principalmente principiológica. Ela foi desenvolvida seguindo a lógica da RGPD, a qual se estabeleceu dessa maneira para facilitar a averiguação do atendimento aos seus requisitos. Conforme dita Peck, "A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido" (2021, p. 50).

São os princípios previstos na LGPD, no art. 6º, I, II, III, IV, V, VI, VII, VIII, IX e X: a finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas (BRASIL, 2018).

Sendo assim, quando na coleta, tratamento, compartilhamento e descarte de dados, deve se interpretar tais princípios, os observando de modo a garantir a:

> (i) finalidade do tratamento;
> (ii) compatibilidade do tratamento com as finalidades informadas ao titular;
> (iii) limitação do tratamento ao mínimo necessário para a realidade de suas finalidades;
> (iv) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma de tratamento;
> (v) garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> (vi) transparência aos titulares;
> (vii) utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais;
> (viii) prestação de contas, pelo agente, da adoção de medidas capazes de comprovar a proteção de dados pessoais. (PECK, 2021, p. 50 e 51)

Além da grande característica principiológica da LGPD, a normativa se baseia em vários requisitos, sendo o fundamental para o caso em estudo, o consentimento, o qual deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular e deve estar vinculado à finalidade apresentada ao titular, quando lhe for requerido.

Há situações, previstas na lei, de exceção ao fornecimento do consentimento do titular, em especial, tem-se excepcionalidade do tratamento para a proteção da vida do titular ou de terceiro, isto é, tal exceção é aplicada majoritariamente em casos de emergência, como em um atendimento médico ambulatorial, no qual faz se necessário a coleta de dados como nome, biometria, endereço, tipo sanguíneo, entre outros.

Uma vez estabelecidos os parâmetros para o cumprimento da lei, reputa-se necessário a compreensão das penalidades quando do seu descumprimento. A LGPD prevê majoritariamente penas no âmbito administrativo, isto é, não há a aplicações de penalidades na esfera cível/penal, à pessoa física, como o dever da indenização por danos morais ou a prisão por condenação criminal, sendo possível apenas a responsabilização e dever de reparação quando o dano for originado de uma atividade de tratamento de dados pessoais pelo controlador ou operador de dados designados, conforme o art. 42 da LGPD (BRASIL, 2018).

Eis algumas das sanções legalmente previstas: advertência com prazo para adoção de medidas corretivas, multa simples de até 2% do faturamento da empresa (por infração cometida), multa diária limitada a R$ 50.000.000,00 (cinquenta milhões de reais), publicização da infração, bloqueio e eliminação dos pessoais referentes ao ato infracional, suspensão parcial do funcionamento do banco de dados a que se refere a infração por até seis meses - prorrogável por igual período -, suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração por até seis meses - prorrogável por igual período - e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, conforme o art. 52 e seus incisos (BRASIL, 2018).

Entretanto, tais sanções possuem aplicações administrativas, ou seja, apenas a autoridade reguladora pode determiná-las. Assim, conforme o art. 55-K da LGPD, a aplicações das sanções previstas na lei competem exclusivamente a Autoridade Nacional de Proteção de Dados - ANPD (BRASIL, 2018).

Quando instituída, a ANPD foi prevista sob uma natureza jurídica transitória, sendo inicialmente um ente vinculado à Presidência da República e depois transformada em uma autarquia, para atuação independente.

No entendimento de Peck quanto à Autoridade:

> A ANPD tem um papel fundamental como elo entre diversas partes interessadas que vão do titular ao ente privado e ao ente público, passando pela necessidade de alinhamento com demais autoridades reguladoras e fiscalizadoras, bem como os três poderes Executivo, Legislativo e Judiciário que deverão continuar a compreender a temática da dinâmica dos dados pessoais em um contexto não apenas nacional, mas principalmente internacional para que o Brasil saiba se posicionar no mercado digital global. (2021, p. 57)

Isto é, a Autoridade precisa se posicionar de modo a fornecer aos interessados a confiança para consultá-la e fornecer informações e também para garantir a efetividade da instituição. De acordo com a Associação Internacional de Profissionais de Privacidade (2020), existem dois perfis de abordagem de atuação das autoridades de proteção de dados pelo mundo, o primeiro possui uma personalidade orientativa e fiscalizatória, enquanto o segundo possui um perfil punitivo e arrecadatório. A ANPD, encaixa-se na descrição do primeiro perfil. Apesar da aplicação de algumas sanções a empresas maiores por vazamento de dados, não há que se falar em um perfil extremamente punitivo ou com vistas à arrecadação.

Contudo, apesar de tal perspectiva, a Autoridade não deixa de aplicar sanções, de modo que todos os responsáveis no tratamento de dados devem adequar-se à legislação. Para isso, exige a adequação de todos os processos da área em questão, por meio de medidas como a implementação de um *compliance* digital, atualização de ferramentas de segurança de dados, revisão de documentos e contratos, melhoria de procedimentos e fluxos internos, auditorias e ainda, alteração da cultura interna das empresas - seja por meio da adequação dos Códigos de Conduta ou por treinamentos regulares.

Para isso, conforme previsão legal, é necessário a atuação do controlador e operador, os quais são responsáveis pela adequação à legislação, por meio de recursos de anonimização, controles de acesso, atualização de procedimentos e políticas e desenvolvimento de treinamentos contínuos.

Ainda que a adequação possa ser realizada mediante a implementação de diversos procedimentos, a LGPD, de fato, exige apenas um determinado documento, o Relatório de Impacto à Proteção de Dados (RIPD). Conforme o art. 5º, XVII, da lei, o RIPD é a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018). Dessa forma, o RIPD descreve um panorama geral das atividades da empresa, com a descrição das áreas, processos, dados coletados e seu efetivo tratamento, assim como todas as medidas aplicáveis aos setores para contenção e mitigação de riscos de vazamento.

Assim, a proteção de dados no âmbito da saúde suplementar, dentro das esferas legislativas e judiciárias são delimitadas nas normativas expostas, enquanto as normas e legislações administrativas e regulamentadoras, são determinadas pelos órgãos reguladores responsáveis.

3 NORMAS E LEGISLAÇÕES REGULAMENTADORAS DA PROTEÇÃO DE DADOS NA SAÚDE SUPLEMENTAR

A área da saúde suplementar compreende o setor privado de saúde, o qual inclui planos, seguros e serviços de saúde, desenvolvidos por pessoas jurídicas de direito privado. Sua operação é regulada pelo poder público, através da agência reguladora Agência Nacional de Saúde Suplementar (ANS), a qual é vinculada ao Ministério da Saúde.

A ANS possui como objetivo a regulamentação, criação, implementação e fiscalização de normas do segmento. Sua função também inclui a garantia da defesa dos interesses públicos, por meio dos seus objetivos.

Nesse sentido, para o trabalho em questão, na pirâmide de Kelsen (2000), abaixo das demais legislações expostas, as Resoluções Normativas n.º 507 e n.º 518, ambas de 2022, da ANS, irão reger a implementação de boas práticas necessárias ao funcionamento dos planos de assistência à saúde, incluindo a necessidade de operações de privacidade aos usuários.

Além disso, os Conselhos Profissionais também são responsáveis pela regulamentação das condutas dos servidores da saúde, quando no atendimento de pacientes e tratamento de seus dados. Inicialmente, a regulamentação ocorria de modo generalista sob as orientações dos Códigos de Ética de cada profissão, mas ao decorrer do tempo e tendo em vista a crescente necessidade de enfoque no tratamento de dados de forma ética, diversas normativas foram surgindo. A exemplo, a Resolução n.º 1.605, de 31 de dezembro de 2009, do Conselho Federal de Medicina - CFM, a qual veda ao médico a disponibilizações de informações de saúde, do prontuário ou ficha médica, sem o consentimento do paciente.

3.1 Normas dos Conselhos de Classe: Conselho Federal de Medicina e do Conselho Federal de Enfermagem

Ainda que o trabalho em questão aborde o caso concreto de um ato lesivo provocado por uma enfermeira, é importante trazer ao estudo as normas dos principais profissionais atuantes na saúde e com maior facilidade de aceso a dados pessoais de saúde, quais sejam, os médicos e enfermeiros.

O Código de Ética Médica - Resolução n.º 2.217, de 27 de setembro de 2018, editado pelo Conselho Federal de Medicina, vincula todos os profissionais médicos habilitados ao exercício da profissão ao seu segmento. Em seu item XI, é possível visualizar a primeira diretriz acerca da garantia do sigilo no exercício da função e da proteção de dados pessoais de pacientes, ao transcrever: “O médico guardará sigilo a respeito das informações de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei.” (CFM,

2019), e reforça tal diretriz o art. 73, quando dita que é vedado ao médico “revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.” (CFM, 2019).

Tais diretrizes determinam a garantia do sigilo profissional, no qual, todos os fatos conhecidos no exercício da função devem ser mantidos em segredo, sem o compartilhamento com qualquer pessoa não autorizada. Contudo, outro meio de conhecimento do estado clínico de um paciente é por meio do seu prontuário ou ficha médica. Tal documento possui diversos dados pessoais e sensíveis, desde o nome, à tipagem sanguínea e a diagnóstico do paciente, de modo que a tratativa de tal documento deve ser a mais rigorosa possível. Para isso, além da previsão do Código de Ética do CFM, o qual dita em seu art. 85 que é vedado ao médico “permitir o manuseio e o conhecimento dos prontuários por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade.” (2021), a Resolução n.º 1.605, de 2009, do CFM, é mais incisiva é veda de forma direta a disponibilizações de informações de saúde, do prontuário ou ficha médica, sem o consentimento do paciente.

Quanto ao exercício da profissão de enfermeiro, estes dispõem do Código de Ética dos Profissionais de Enfermagem - Resolução n.º 564, de 06 de dezembro de 2017, do Conselho Federal de Enfermagem - Cofen. Dessa forma, dispõe o Código de forma expressa quanto ao dever de sigilo do enfermeiro no exercício da profissão:

> Art. 52 Manter sigilo sobre fato de que tenha conhecimento em razão da atividade profissional, exceto nos casos previstos na legislação ou por determinação judicial, ou com o consentimento escrito da pessoa envolvida ou de seu representante ou responsável legal.
>
> § 1º Permanece o dever mesmo quando o fato seja de conhecimento público e em caso de falecimento da pessoa envolvida.
>
> § 2º O fato sigiloso deverá ser revelado em situações de ameaça à vida e à dignidade, na defesa própria ou em atividade multiprofissional, quando necessário à prestação da assistência.
>
> [...] (COFEN, 2017).

O sigilo quanto às circunstâncias que dizem respeito ao paciente deve ser absoluto, sendo flexibilizado apenas mediante as hipóteses do Código, de modo a garantir a proteção dos direitos fundamentais dos pacientes.

3.2 Resolução Normativa n.º 507, de 30 de março de 2022, da Agência Nacional de Saúde Suplementar

A Resolução Normativa n.º 507, de 30 de março de 2022 - RN 507/22, dispõe sobre o Programa de Acreditação de Operadoras de Planos Privados de Assistência à Saúde. Conforme o art. 2º da RN, o Programa de Acreditação de Operadoras:

> é uma certificação de boas práticas em gestão organizacional e em gestão em saúde, de caráter voluntário, realizado por Entidades Acreditadoras, cujo objetivo é a qualificação da prestação dos serviços, induzindo a mudança no modelo de atenção à saúde existente, propiciando uma melhor experiência para o beneficiário. (ANS, 2022)

Como exposto, a ANS possui caráter regulamentador para as operadoras de saúde privada, nesse sentido, a RN 507 deve ser seguida por todas, no caso de sua inobservância não há a previsão de atos punitivos, mas sim a privação de atos de bonificação.

Conforme o art. 30 da referida RN, as operadoras acreditadas, isto é, aprovadas conforme seus requisitos, receberão a bonificação corresponde ao nível atingido no índice de Desempenho da Saúde Suplementar – IDSS[1] o Programa de Qualificação, além disso, conforme as demais disposições da resolução é possível a obtenção de benefícios como: redução da exigência mensal da margem de solvência e redução de fatores de capital regulatório (ANS, 2022).

Ainda que a norma não seja obrigatória, é do melhor interesse para todas as operadoras do ramo a obtenção do credenciamento, uma vez demonstrada os benefícios para o negócio, além do aumento do valor da empresa perante o mercado externo, posto que o atendimento às normativas da ANS demonstra a saúde do negócio e a preocupação com a sustentabilidade das atividades desenvolvidas.

Para uma melhor compreensão da importância da adequação das operadoras às RN's, é importante estar ciente que operadoras de planos de saúde adotam uma lógica baseada na teoria do risco, típica do setor securitário. Assim, o valor da mensalidade é determinado com base na probabilidade de utilização dos serviços de saúde, o que influencia diretamente na margem de lucro da empresa. Dessa forma, para a obtenção das acreditações que irão trazer diversos benefícios econômicos, as operadoras de saúde devem atender a uma série de requisitos e itens

[1] O Índice de Desempenho da Saúde Suplementar da Operadora - IDSS consiste na avaliação sistemática do desempenho da operadora, expresso por um conjunto de indicadores, que representam atributos esperados no desempenho de áreas relacionadas ao setor de saúde suplementar. Os indicadores avaliados são agregados em dimensões que representam a qualidade em atenção à saúde, garantia de acesso, sustentabilidade no mercado e gestão de processos e regulação. Para cada dimensão é atribuído um índice de desempenho e o IDSS da operadora é calculado a partir do somatório dos índices de desempenho da dimensão, de forma ponderada. O IDSS varia de zero a um (0 a 1) e a nota de cada operadora é enquadrará em uma das cinco faixas de avaliação por ordem crescente de desempenho (0 a 0,19; 0,20 a 0,39; 0,40 a 0,59; 0,60 a 0,79; 0,8 a 1) (ANS, 2022).

de verificação, os quais são aferidos de forma rígida por uma comissão de auditoria, a qual também é escolhida de forma igualmente rigorosa.

Contudo, para o estudo em questão faz se importante a menção ao item 1.4.2, da referida RN, o qual prevê que a operadora de saúde deve possuir um plano diretor de tecnologia da informação que contemple a existência de mecanismos tecnológicos para proteção de informações sensíveis de cadastro e transações operacionais, isto é, deve-se adotar técnicas de criptografia para o tratamento de dados sensíveis, evitando seu vazamento.

Em acréscimo, o item 1.5.2 dita acerca da importância do estabelecimento de um termo de confidencialidade na operadora, de modo que todos os envolvidos devem assiná-lo. Na interpretação do item dita a resolução de forma clara quanto aos deveres vinculados pelo termo:

> guardar sigilo e zelar pela privacidade das informações confidenciais a que tiver acesso, sem divulgá-las para pessoas não autorizadas; estar ciente de que as responsabilidades dispostas no documento perdurarão inclusive após a cessação do vínculo contratual com a empresa e abrangem as informações de propriedade da organização. Para ser efetivo, deve contemplar menção à responsabilidade dos usuários pelas consequências legais, inclusive por danos materiais ou financeiros, devidamente comprovados, em virtude da não observância dos itens elencados. (ANS, 2022)

Já no item 1.5.3, há a previsão do armazenamento de informações cadastrais e clínicas para garantir sua disponibilidade, integridade e confidencialidade. Tais padrões derivam da norma ISO/IEC 17799:2005 (atualizada pela ISO/IEC 27002), a da sigla *CIA* (*Confidentiality, Integrity and Availability*) - Confidencialidade, Integridade e Disponibilidade. Ou seja, todos os dados tratados devem ser disponibilizados para seu uso legítimo (aquele para o qual o titular permitiu o uso), íntegros, de modo a não serem modificados, mantendo as características fornecidas pelo titular e confidenciais: restritos apenas aos legitimados para acessá-los (mediante autorização expressa do titular, conforme a LGPD) (ANS, 2022).

Logo, a resolução estabelece critérios específicos acerca do tratamento de dados dentro do âmbito da saúde suplementar, ainda que, em uma primeira análise, de forma mais incisiva quanto ao tratamento nas plataformas digitais.

3.3 Resolução Normativa n.º 518, de 29 de abril de 2022, da Agência Nacional de Saúde Suplementar

A Resolução Normativa n.º 518, de 29 de abril de 2022 - RN n.º 518/22, dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de plano de assistência à saúde.

Contrariamente à RN n.º 507/22 a RN n.º 518/22 não dispõe acerca do tratamento de dados na saúde ou sequer acerca de medidas de segurança da informação. Entretanto, a norma

detém grande importância para as operadoras de saúde por ser obrigatória para as operadoras de grande e médio portes, e por ser mais um meio de obtenção de benefícios regulatórios, uma vez que a adequação a esta concede o benefício da redução de fatores de capital regulatórios.

Para a análise do enquadramento das operadoras à norma é necessário o envio de um Relatório anual de Procedimentos Previamente Acordados, elaborado por um auditor independente, tendo como base os dados do exercício antecedente referentes aos processos de governança, gestão de riscos e controles internos das operadoras, consoante dispõem os artigos 11 e 12 da Resolução (ANS, 2022).

Para o trabalho em questão, faz-se necessário a menção ao Anexo III da Resolução, o qual prevê as práticas avançadas e estrutura de governança, gestão de riscos e auditoria interna a serem verificadas, para operadoras com modelos próprios de capital baseado em riscos. Na estrutura de conduta ética, o item 1.3 prevê que a operadora deve "estabelecer regras de conduta e de ética revisadas e aprovadas formalmente pelo conselho de administração ou equivalente, disponibilizando-as às partes interessadas." (2022, p.1), e no item 1.4 que:

> A operadora deve possuir programa de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta internos, com vistas à prevenção dos atos previstos na Lei nº 9.613, de 3 de março de 1998; de operações vedadas pelo art. 21 da Lei nº 9.656, de 3 de junho de 1998, e de atos lesivos à administração pública nacional ou estrangeira, conforme o disposto na Lei nº 12.846, de 1 de agosto de 2013. Os programas de treinamento nesses temas deverão ser disponibilizados e implementados, definindo-se, pelo menos, público alvo e periodicidade. (ANS, 2022, p.1)

Dessa forma, a normativa regula a atuação das operadoras de modo a garantir que todas as suas operações ocorram de forma ética, prezando pela proteção dos direitos fundamentais da Constituição Federal, como a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, como um direito fundamental, sob a forma do art. 5º, X e o direito à proteção de dados, no também no art. 5º, LXXIX (BRASIL, 1988).

3.4 Lei n.º 12.846, de 1º de agosto de 2013 – Lei Anticorrupção

Retornando ao estudo das legislações brasileiras e para o desenvolvimento da compreensão da temática, faz-se necessário o estudo da Lei Anticorrupção, a qual deriva de um contexto histórico intenso.

No século XX, com o desenvolvimento dos modelos de negócios e a grande onda do sistema capitalismo, também se desenvolveram os modelos ilícitos de negócios, isto é, os atos de corrupção. Como meio de combate à prática de tais atos, o Estados Unidos da América (EUA), em 1977, promulgou a *Foreign Corrupt Practices Act – FCPA* (ESTADOS UNIDOS DA AMÉRICA), um Ato que passou a exigir das empresas que operam na Bolsa de Valores de

Nova York a adoção de um conjunto de medidas voltadas a evitar e punir fraudes e atos de corrupção. O Ato norte-americano aplicou-se a pessoas físicas e jurídicas que operassem em seu território ou vinculado a ele, de modo que a normativa inspirou a adoção dos demais países do globo aos seus próprios modelos, posto que sua inobservância geraria uma barreira econômica.

Em um primeiro momento, o Brasil adere ao Ato por meio da adesão à Convenção sobre a Luta Contra a Corrupção de Agentes Públicos Estrangeiros nas Transações Comerciais, da Organização para o Cooperação e Desenvolvimento Econômico. Com a ratificação da convenção, o Ato é incorporado ao ordenamento jurídico com força de lei ordinária, sendo assim, obrigatório a todos.

Em adição ao arcabouço normativo, a Lei n.º 12.846 de 1º de agosto de 2013, conhecida como Lei Anticorrupção, versa sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos lesivos que sejam cometidos contra a administração pública, nacional ou estrangeira.

Conforme interpretação dos artigos 2º e 3º da Lei, as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, contudo, não se exclui da responsabilidade individual os dirigentes, administradores, ou qualquer pessoa natural que seja autora, coatora ou partícipe do ato ilícito (BRASIL, 2013).

Além de apresentar o caráter punitivo, por meio da aplicação dos artigos 2º e 3º da Lei em comento a quem infringir quaisquer dos atos elencados, há também a previsão da necessidade de implementação de uma série de medidas como forma de combate, prevenção e atenuante da responsabilização, as quais são implementadas por meio do Programa de Integridade (BRASIL, 2013).

3.5 *Compliance* Empresarial

Afunilando ao tema em análise, em que pese a existência de todas as legislações e normativas apresentadas, faz-se necessário a existência de um instrumento de aplicação destas. Assim, surgiu o *compliance*, como meio de aplicabilidade de medidas de prevenção de sanções, por meio da disseminação de uma cultura de ética.

O termo em inglês *compliance*, deriva do verbo "*to comply*", isto é, estar em acordo, conformidade ou em obediência. Na visão de Mendes e Carvalho:

> a palavra compliance vem do inglês to comply, que significa cumprir. De forma resumida, um programa de compliance é aquele que busca o cumprimento da lei. [...] Um programa de compliance visa estabelecer mecanismos e procedimentos que tornem o cumprimento da legislação parte da cultura corporativa. Ele não pretende, no entanto, eliminar 11 completamente a chance de ocorrência de um ilícito, mas sim

> minimizar as possibilidades de que ele ocorra, e criar ferramentas para que a empresa rapidamente identifique sua ocorrência e lide da forma mais adequada possível com o problema. (2017, p. 26)

Pauseiro e Paiva, explicam de forma clara a importância e aplicabilidade do *compliance* nas empresas, atuando como pilar para o desenvolvimento de uma empresa íntegra e também:

> [...] o compliance é adotado pelas corporações como instrumento de combate à corrupção, de atenuante da responsabilidade da empresa e dos administradores em caso de práticas antiéticas, de combate a fraudes internas e de manutenção da boa imagem e reputação, sendo um instrumento para evitar que a empresa seja afetada por condutas antiéticas. (2019, p. 15).

O *compliance*, ainda que extremamente benéfico e necessário nas relações comerciais e na cultura diária, não é uma área obrigatória para todas as empresas no Brasil. Ainda que a Lei Anticorrupção preveja a implementação de medidas éticas e as resoluções da ANS requeiram o cumprimento de uma série de itens, inexiste no país uma legislação regulamentadora do modelo de *compliance* a ser seguido.

Dessa forma, o ato comum entre as empresas que buscam implementá-lo é a criação de um setor destinado ao *compliance*, visando: obedecer às normas regulamentadoras do seu modelo de negócio (como as da ANS para as operadoras de saúde) e as demais legislações brasileiras que versem acerca de necessidade de adequação e combate a atos lesivos como: a Lei Anticorrupção - Lei n.º 12.846/2013, a Lei de Combate a Lavagem de Dinheiro - Lei n.º 9.613/1998, Lei de Licitações - Lei n.º 14.133/2021 e a Lei Geral de Proteção de Dados - Lei n.º 13.709/2018.

Tal área é essencial, uma vez que de acordo com a Organização de Transparência Internacional (2024), em 2024 o Brasil registrou 34 pontos no Índice de Percepção da Corrupção, a pontuação de um país pode variar entre 0 (percebido como muito corrupto) a 100 (percebido como muito íntegro), sendo esta a pior nota do país desde o início do índice em 2012.

Dessa forma, o *compliance* atua adequando as mais diversas normas de combate à corrupção e condutas antiéticas, entrelaçando-se para atender a normativas legislativas e regulatórias, para que os usuários desenvolvam um senso de confiança na empresa, e assim, aumente o valor dela no mercado.

Para Giddens:

> A confiança pode ser definida como a crença na credibilidade de uma pessoa ou sistema, tendo em vista um dado conjunto de resultados ou eventos, em que esta crença expressa uma fé na probidade ou amor de um outro, ou na correção de princípios abstratos (conhecimento técnico). (1990, p. 40)

Assim, desenvolvendo a confiança do usuário, desenvolve-se a credibilidade da empresa no mercado, aumentando seu valor e margem de adesão.

3.5.1 *Compliance* Digital

O *compliance digital* é um seguimento do *compliance* originário, e o meio pelo qual as empresas implementam as medidas de LGPD em uma empresa e abrangem suas defesas no âmbito da rede interna e externa.

Conforme mencionado anteriormente, a LGPD formalmente requer apenas um documento: o RIPD. Contudo, para a produção do RIPD é necessário o desenvolvimento de uma série de procedimentos encabeçados pelo *Data Protection Oficcer* - DPO ou Encarregado de Dados, mas com a participação de todos os setores das empresas.

O Encarregado é, segundo o art. 5º, VIII, da LGPD, a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (BRASIL, 2018). Seus deveres são a responsabilidade pela comunicação entre a empresa, os titulares e a ANPD - seja na resposta à incidente ou em consulta -, a adequação da empresa à lei, capacitação e orientação e monitoramento contínuo das atividades.

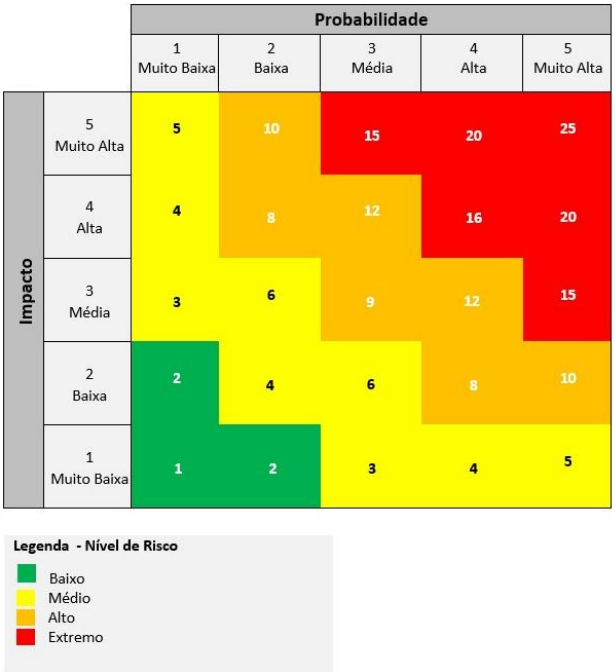
Assim, formalmente, faz-se necessário o RIPD. Para a produção do RIPD e implementação da LGPD, o Encarregado irá seguir um *script* padrão que pode ser implementado pela maioria das empresas que desejam se adequar a LGPD (CUNHA, PEREIRA, TIMOTEO, BARBOSA, *et.al*, 2021), iniciando pela implementação de um comitê de proteção de dados, contendo os principais setores de uma empresa como: gestão de pessoas, tecnologia da informação, financeiro, jurídico, marketing, *compliance* e a alta administração. O comitê será responsável por acompanhar todas as etapas de adequação a LGPD e agir para garantir o engajamento de todos os interessados, contribuir no desenvolvimento de políticas ou documentos e também aprová-los.

A seguir, é necessário realizar um mapeamento de dados, o *Data Mapping*, o qual é feito com todos os setores que integram a empresa, determinando: quais dados pessoais e sensíveis são coletados, tratados, compartilhados e excluídos, quem obtém acesso a estes, por quanto tempo são armazenados, sistemas em que estes trafegam (nacionais ou internacionais) e para quais fins são necessários. Tudo isso possui o propósito de avaliar a maturidade da empresa quando ao tratamento de dados, definindo quais áreas possuem as maiores falhas de segurança e como os dados estão sendo tratados, determinando quais são realmente pertinentes

para o desenvolvimento do negócio e sob a ótica dos princípios da LGPD (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).

Com o mapeamento de dados prontos, é possível encaminhá-lo para os responsáveis pela segurança da informação na empresa. Com o documento, os capacitados conseguem ter uma visualização de quais processos e sistemas são mais suscetíveis de ataques externos ou de vazamento por funcionários e, assim, gerarão os relatórios de avaliação de segurança da informação.

Concluídos tais documentos, e mediante a contraprestação constante perante a comissão de LGPD, é possível obter um panorama dos riscos da empresa, sejam de segurança da informação, sejam de LGPD. Dessa forma, o Encarregado deve produzir uma matriz de risco, a qual serve para definir os maiores riscos para a organização baseado em: qual seria o seu impacto para a empresa (financeiro, jurídico e reputacional) e sua probabilidade de ocorrer (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).



Fonte: Tribunal Regional do Trabalho da 10ª Região.

Por meio da matriz de riscos é possível gerar o RIPD. O RIPD é o documento responsável por identificar, analisar e mitigar riscos referentes aos dados utilizados por uma empresa (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021). Tal Relatório deve ser constantemente atualizado, uma vez que os processos de uma empresa são mutáveis e este é o principal documento para a LGPD. Sempre que entender necessário ou em caso de um incidente de vazamento, a ANPD deve solicitar o RIPD (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2023).

Com uma perspectiva definida da organização quanto aos dados coletados, seu uso e seus riscos, deve-se elaborar a Política de Proteção de Dados, de modo a constar para todos os interessados em todas as plataformas da empresa, devendo ser encontrada com fácil acesso. A Política deve definir padrões rigorosos de segurança para o tratamento de dados pessoais, garantindo que desde a admissão de empregados ao descarte de qualquer material com dados pessoais, haja a observância às normas de proteção de dados (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).

Por fim, não basta que a adequação de todos os itens sem a conscientização de todos os envolvidos na empresa, desde a alta administração aos terceirizados. Para isso, é necessário treinamentos constantes com cada público, sinalizando os riscos de cada operação desenvolvida no setor e das sanções cabíveis no caso de vazamentos (CONTROLADORIA-GERAL DO ESTADO DO PARANÁ, 2021).

3.6 Programa de Integridade

No âmbito da Saúde Suplementar tem-se a implementação de Programas de Integridade, em consonância com o disposto nas Resoluções Normativas da ANS, Decreto n.º 11.129/22 e a LGPD. Dessa forma, há a minimização dos riscos de vazamento de dados e, por consequência, da violação dos direitos à privacidade dos titulares.

Ainda que o *compliance* não seja obrigatório, a instauração de um Programa de Integridade é, para as empresas que buscam determinados benefícios ou participar de determinadas transações. Para isso, muitas empresas implementam um setor de *compliance*, o qual é responsável por instituir o Programa de Integridade.

Sob a ótica de Zolandeck, o Programa traz apenas benefícios:

> O programa de integridade, que consiste no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades, foi regulamentado no artigo 41 do Decreto já referido. Bem implantado, minimizará os efeitos da corrupção, alçando a empresa à condição de agente de transformação, a partir de uma nova ou modificada cultura empresarial/organizacional, ancorada no princípio da confiança. (2017, p. 56)

Assim, o Programa de Integridade, regido pelo Decreto n.º 11.129, de 11 de julho de 2022, em seu art. 56, é definido como:

> conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes, com objetivo de:
> I - prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira; e
> II - fomentar e manter uma cultura de integridade no ambiente organizacional.
> Parágrafo único. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e os riscos atuais das atividades de cada

> pessoa jurídica, a qual, por sua vez, deve garantir o constante aprimoramento e a adaptação do referido programa, visando garantir sua efetividade. (BRASIL, 2022)

Para isso, conforme o entendimento de Porto (2020), é necessária a definição de pilares básicos, bem alicerçados e distribuídos dentro da empresa, sendo subdivididos da seguinte forma:

1º) Engajamento e comprometimento da Alta Administração: devem os administradores, conselheiros, diretores e todos em posição de liderança demonstrarem engajamento e comprometimento com as normas reguladoras, seja através da participação ativa em atividades de disseminação de condutas, seja na aprovação de códigos internos e medidas de combate.

2º) Avaliação de riscos: é dever de toda organização uma avaliação periódica para o conhecimento de potenciais riscos e seus impactos. Com isso, é possível traçar um plano de ação, seja para o combate ou para a minimização de impactos.

3º) Código de Conduta e políticas: a implementação de um Código de Conduta e demais políticas como, Política de Privacidade, Política de Segurança da Informação, Política de *Compliance*, são essenciais, pois estas determinam as diretrizes norteadoras dos comportamentos dentro da organização. Sua criação gera um vínculo entre as normas e legislativas externas com os deveres internos de cada participante da organização, desde o colaborador até o presidente.

4º) Controles internos: dizem respeito ao estabelecimento de mecanismos e estratégias para o controle das atividades internas e avaliações periódicas para a melhoria dos processos.

5º) Treinamento e comunicação: mediante a instalação de todos os pilares, o treinamento e os produtos de comunicação serão o meio mais eficiente para a disseminação das normativas e introdução de uma cultura de ética, por meio do aprendizado acerca do *compliance*.

6º) Canal de denúncias: item essencial para o controle e quantificação da efetividade do compliance na organização. É necessário para além de coibir medidas que vão de encontro com quaisquer normativas, como também para aferir pontos de melhoria.

7º) Investigações internas: com o recebimento de denúncias, é necessário o tratamento e investigação para atestar sua veracidade. Dessa forma, as investigações devem ser conduzidas por um profissional capacitado e externo à organização, como forma de evitar qualquer imparcialidade.

8º) *Due dilligence*: o procedimento diz respeito à avaliação de determinados aspectos de parceiros de negócios. Seu objetivo é verificar se tal parceiro também está adequado a medidas de compliance, legislações, e quais riscos tal parceria possa oferecer.

9º) Auditoria e monitoramento: para a garantia da implantação e execução perfeita dos demais pilares faz-se necessário auditorias e sistemas de monitoramento, de modo a detectar quaisquer falhas nos processos e executar melhorias.

Apesar deste modelo base, implantado em diversas empresas, também não há na normativa brasileira uma determinação específica de como o Programa de Integridade deve ser executado, definindo quais pilares devem ou não existir. Todavia, o Decreto que o regulamento determina parâmetros para a avaliação da existência e de sua aplicação nas organizações, são eles:

> I - comprometimento da alta direção da pessoa jurídica, incluídos os conselhos, evidenciado pelo apoio visível e inequívoco ao programa, bem como pela destinação de recursos adequados;
>
> II - padrões de conduta, código de ética, políticas e procedimentos de integridade, aplicáveis a todos os empregados e administradores, independentemente do cargo ou da função exercida;
>
> III - padrões de conduta, código de ética e políticas de integridade estendidas, quando necessário, a terceiros, tais como fornecedores, prestadores de serviço, agentes intermediários e associados;
>
> IV - treinamentos e ações de comunicação periódicos sobre o programa de integridade;
>
> V - gestão adequada de riscos, incluindo sua análise e reavaliação periódica, para a realização de adaptações necessárias ao programa de integridade e a alocação eficiente de recursos;
>
> VI - registros contábeis que reflitam de forma completa e precisa as transações da pessoa jurídica;
>
> VII - controles internos que assegurem a pronta elaboração e a confiabilidade de relatórios e demonstrações financeiras da pessoa jurídica;
>
> VIII - procedimentos específicos para prevenir fraudes e ilícitos no âmbito de processos licitatórios, na execução de contratos administrativos ou em qualquer interação com o setor público, ainda que intermediada por terceiros, como pagamento de tributos, sujeição a fiscalizações ou obtenção de autorizações, licenças, permissões e certidões;
>
> IX - independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e pela fiscalização de seu cumprimento;
>
> X - canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e mecanismos destinados ao tratamento das denúncias e à proteção de denunciantes de boa-fé;
>
> XI - medidas disciplinares em caso de violação do programa de integridade;

> XII - procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados;
>
> XIII - diligências apropriadas, baseadas em risco, para:
>
> a) contratação e, conforme o caso, supervisão de terceiros, tais como fornecedores, prestadores de serviço, agentes intermediários, despachantes, consultores, representantes comerciais e associados;
>
> b) contratação e, conforme o caso, supervisão de pessoas expostas politicamente, bem como de seus familiares, estreitos colaboradores e pessoas jurídicas de que participem; e
>
> c) realização e supervisão de patrocínios e doações;
>
> XIV - verificação, durante os processos de fusões, aquisições e reestruturações societárias, do cometimento de irregularidades ou ilícitos ou da existência de vulnerabilidades nas pessoas jurídicas envolvidas; e
>
> XV - monitoramento contínuo do programa de integridade visando ao seu aperfeiçoamento na prevenção, na detecção e no combate à ocorrência dos atos lesivos previstos no art. 5º da Lei nº 12.846, de 2013. (BRASIL, 2022)

É possível visualizar como o sistema de pilares de Porto engloba bem os principais parâmetros do decreto, facilitando sua aplicação nas empresas.

Traçando uma referência à RN 507/2022, seu item 1.2.11 determina como dever para a bonificação das Operadoras:

> A Operadora possui órgão interno ou estrutura de *compliance* responsável por implementar, disseminar, treinar e atualizar o código de conduta da empresa e avaliar os desvios de conduta e conflitos de interesse. (ANS, 2022)

Ainda, seu item 1.2.12 determina como dever que a "Operadora possui Política/Diretrizes ou um Programa de Integridade formalmente estabelecido e documentado." (ANS, 2022). E também, o item 1.2.17, que:

> a Política/Diretrizes ou o Programa de Integridade é parte integrante da rotina da Operadora e atua de maneira integrada com outras áreas correlacionadas tais como recursos humanos, departamento jurídico, auditoria interna, departamento contábil e financeiro. (ANS, 2022)

Ou seja, o Programa de Integridade, bem implementado pelo *compliance*, e com o funcionamento dos pilares previstos por Porto (2020) é visto como um requisito essencial para as operadoras de saúde que desejam tanto a bonificação regulatória, quanto a demonstração da adesão de boas práticas de mercado.

Para além disso, a demonstração do atendimento aos requisitos das RN's e sua consequente acreditação, implicam na comprovação de que a empresa está adequada aos padrões rigorosos do seu órgão regulador. De modo a também comprovar que atua para garantir

os melhores interesses de seus usuários e aplicação de todas as medidas necessárias para a sua proteção.

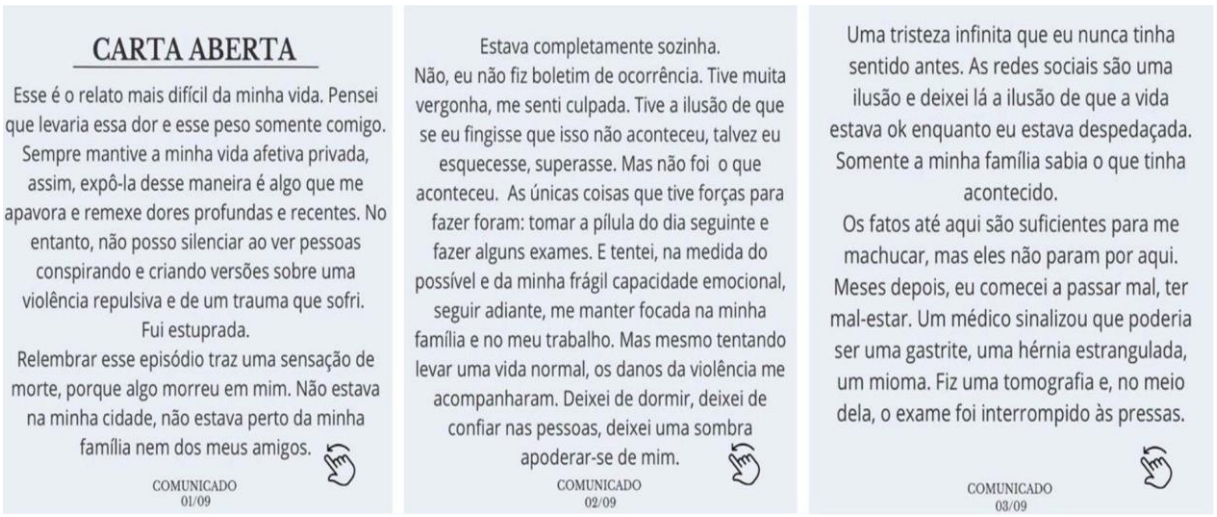
4 O CASO KLARA CASTANHO E O VAZAMENTO DE DADOS NO ÂMBITO DA SAÚDE SUPLEMENTAR

A atriz brasileira Klara Forkas Gonçalez Castanho, popularmente conhecida como apenas Klara Castanho, traçou uma trajetória de trabalho desde a sua infância, atuando em novelas da Rede Globo. Em 2022, teve sua privacidade invadida, violada e exposta para todo o mundo, por meio da internet.

Segundo o jornal Folha de São Paulo (2022), toda a situação iniciou-se quando o jornalista Matheus Baldi, em 24 de maio de 2022, realizou um post na rede social Instagram, dizendo que a atriz teria dado à luz uma criança, enquanto Klara havia se retirado da exposição pública para manter a gravidez em segredo. A pedido da atriz, o jornalista tirou a publicação do ar, ainda que tal informação já tivesse sido disseminada nas redes.

Em 16 de junho de 2022, conforme o Canal The Noite (2022), o jornalista Leo Dias, em participação ao programa televisivo “The Noite”, do apresentador Danilo Gentili, abordou indiretamente o caso, mencionando um “ato maldoso” de uma atriz conhecida. A seguir, em 23 de junho de 2022, a apresentadora Antônia Fontenelle ditou em uma transmissão ao vivo pela internet que uma atriz da Globo, de 21 anos, havia engravidado, escondido a gravidez, dado à luz e entregado o filho, se recusando a vê-lo e pedido para apagar sua entrada ao hospital (FONTENELLE, 2022). Depois disso, Klara se manifestou pela primeira vez sobre o assunto.

Em uma carta aberta, em 25 de junho de 2022, por meio de seu perfil na rede social Instagram, a atriz expôs sua versão do fato ocorrido:



CARTA ABERTA

Esse é o relato mais difícil da minha vida. Pensei que levaria essa dor e esse peso somente comigo. Sempre mantive a minha vida afetiva privada, assim, expô-la desse maneira é algo que me apavora e remexe dores profundas e recentes. No entanto, não posso silenciar ao ver pessoas conspirando e criando versões sobre uma violência repulsiva e de um trauma que sofri.

Fui estuprada.

Relembrar esse episódio traz uma sensação de morte, porque algo morreu em mim. Não estava na minha cidade, não estava perto da minha família nem dos meus amigos.

COMUNICADO 01/09

Estava completamente sozinha.

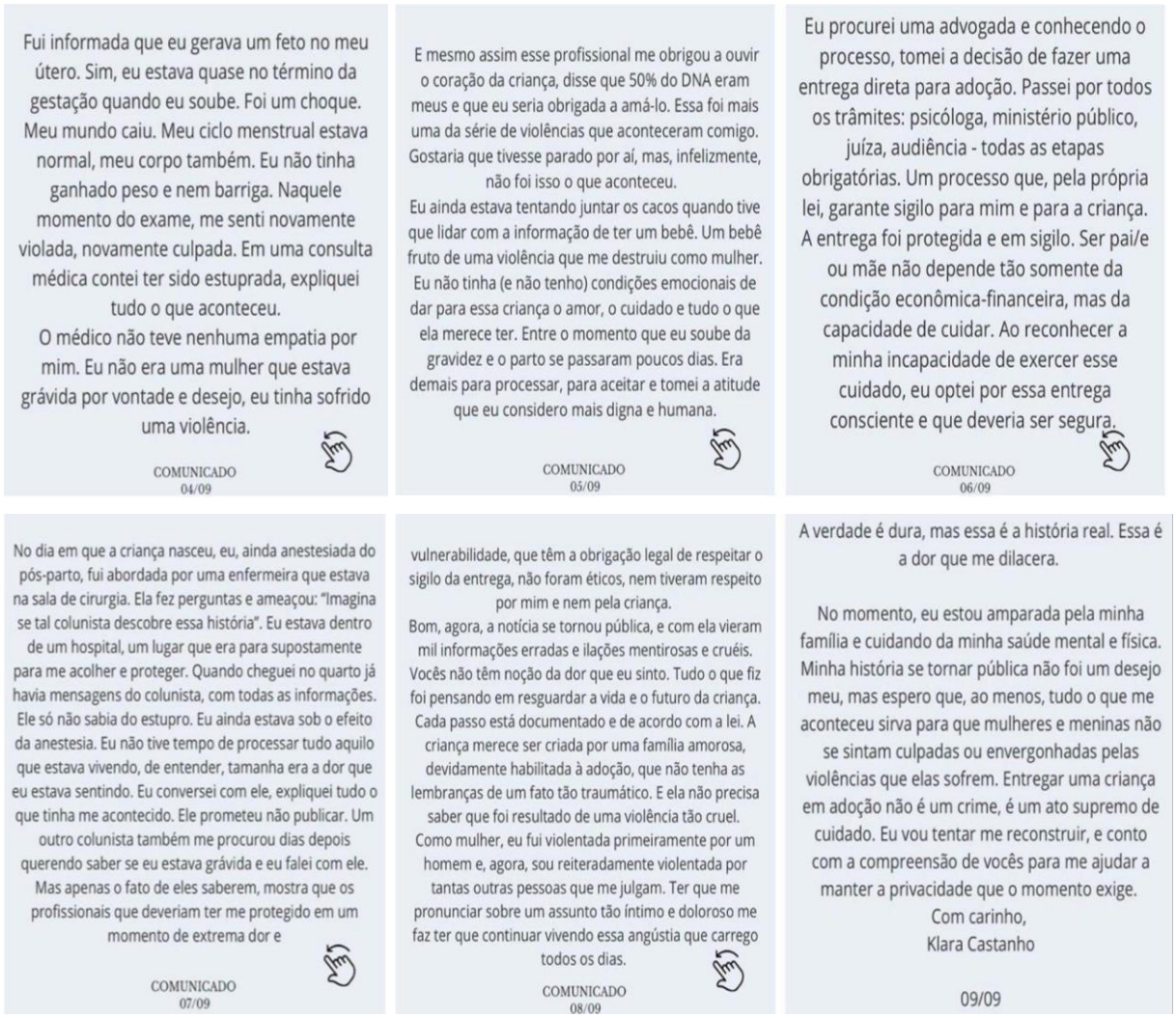
Não, eu não fiz boletim de ocorrência. Tive muita vergonha, me senti culpada. Tive a ilusão de que se eu fingisse que isso não aconteceu, talvez eu esquecesse, superasse. Mas não foi o que aconteceu. As únicas coisas que tive forças para fazer foram: tomar a pílula do dia seguinte e fazer alguns exames. E tentei, na medida do possível e da minha frágil capacidade emocional, seguir adiante, me manter focada na minha família e no meu trabalho. Mas mesmo tentando levar uma vida normal, os danos da violência me acompanharam. Deixei de dormir, deixei de confiar nas pessoas, deixei uma sombra apoderar-se de mim.

COMUNICADO 02/09

Uma tristeza infinita que eu nunca tinha sentido antes. As redes sociais são uma ilusão e deixei lá a ilusão de que a vida estava ok enquanto eu estava despedaçada. Somente a minha família sabia o que tinha acontecido.

Os fatos até aqui são suficientes para me machucar, mas eles não param por aqui. Meses depois, eu comecei a passar mal, ter mal-estar. Um médico sinalizou que poderia ser uma gastrite, uma hérnia estrangulada, um mioma. Fiz uma tomografia e, no meio dela, o exame foi interrompido às pressas.

COMUNICADO 03/09



Fonte: Instagram, 2022.

Com a publicação da atriz, no mesmo dia, o jornalista Leo Dias expôs uma matéria, no Portal Metrópoles, com o título: "Estupro, gravidez indesejada e adoção: a verdade sobre Klara Castanho". Na matéria, o jornalista expôs o nome e imagem da atriz e dados do nascimento da criança. Com a repercussão imediata do caso, a diretora de redação do Portal determinou a retirada da matéria do ar e o jornalista Leo Dias apresentou uma carta aberta pedindo perdão pelo ato de exposição, conforme informa o Fantástico (2022).

O Hospital Brasil, pertencente ao grupo hospitalar privado da Rede D'OR São Luiz e local onde ocorreu o parto e o vazamento de dados, manifestou-se demonstrando solidariedade à atriz e informando que iniciaria um processo interno de investigação dos fatos para a aplicação de todas as medidas cabíveis (Portal G1, 2022).

O Cofen também se manifestou, comprometendo-se em investigar o acontecido e penalizar a profissional da categoria que estivesse envolvida com o caso, tendo em vista a clara violação da privacidade de Klara e do processo sigiloso de entrega voluntária para adoção

(Estadão, 2023). Alguns meses depois o Conselho Regional de Enfermagem de São Paulo (COREN-SP) arquivou o processo por ausência de provas, ditando que:

> [...] seguiu todos os ritos processuais, solicitou documentos à instituição hospitalar e convocou os profissionais do plantão à época, porém não constatou a participação de nenhum profissional de enfermagem em relação ao vazamento de quaisquer informações sigilosas de pacientes, o que levou ao arquivamento do processo. O fato de o processo ter sido arquivado por ausência de provas comprobatórias do envolvimento da enfermagem não significa que o Coren-SP afirme categoricamente que ele não ocorreu. Por isso, permanece à disposição da atriz, caso seja de seu interesse prestar diretamente ao conselho informações que possam complementar as investigações realizadas até o momento. (2022)

Quanto à ANPD e à ANS, inexistem indícios de que as agências reguladoras tenham iniciado uma investigação acerca do caso, ou que tenham sido provocadas a agir, ainda que a repercussão do caso tenha sido tão grande, tornando-o tão conhecido no Brasil.

No tocante às ações judiciais promovidas pela atriz, o acesso aos autos para a realização do estudo em questão foi negado pela serventuária da 8ª Vara Cível de Santo André, São Paulo, tendo em vista a natureza sigilosa dos autos, ainda que o pedido de acesso tenha sido pautado na função plenamente acadêmica.

Dessa forma, em consulta a portais de notícias brasileiras, aferiu-se apenas que o processo movido em face do Hospital Brasil resultou na condenação em R$ 200.000.00 (duzentos mil reais) por danos morais, devido ao vazamento de informações sobre a gravidez da atriz. Em sede de 1º grau, a 8ª Vara Cível de Santo André reconheceu a responsabilidade da empresa no caso, atribuindo o vazamento de dados como uma falha grave de conduta dos funcionários do hospital, infringindo normas constitucionais e da LGPD (MIGALHAS, 2024).

A priori, a condenação havia sido arbitrada em R$ 1.000.000,00 (um milhão de reais), sendo reduzida para R$ 200.000.00 (duzentos mil reais) quando reformada pela 1ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo (MIGALHAS, 2024). No acórdão, o relator do caso, o desembargador Francisco Loureiro, destacou "a clara violação do sigilo profissional, enfatizando a responsabilidade do hospital em proteger os dados de saúde da paciente." (MIGALHAS, 2024).

Isto posto, no capítulo a seguir do trabalho, desenvolver-se-á uma compreensão estendida das normas violadas, os fundamentos para tal e a aplicabilidade das sanções entendidas como cabíveis.

Tendo em vista todo o contexto que envolve o caso, este trabalho foi motivado para estudá-lo, de modo a verificar quais seriam as sanções e penalidades possíveis para o vazamento e como estas poderiam ter sido evitadas e diminuídas, mediante a implementação de um programa de *compliance* efetivo e presente no dia a dia dos funcionários.

4.1 Análise do Caso Sob a Luz da Legislação Brasileira na Perspecitiva Judicial

Uma vez exposta todas as matérias de fato e direito quanto ao caso, permite-se a realização da análise dos fatos sob a luz das normas e legislações brasileiras.

Iniciando a análise pela mesma lógica de organização das normas Kelseniana, analisam-se os direitos constitucionais violados. Para a Constituição Federal de 1988, na forma do art. 5º, X, é vedado a violação da intimidade, vida privada, honra e imagem das pessoas, assim como é garantido o direito a proteção dos dados pessoais, conforme o inciso LXXIX do mesmo artigo (BRASIL, 1988).

Com o vazamento da história de entrega do bebê para adoção, do prontuário médico dele e da identidade da atriz, é possível afirmar que houve a violação de todos os direitos supramencionados. Isto é, a divulgação sem o consentimento de Klara violou sua garantia de proteção da intimidade e vida privada, tendo sua vida exposta por diversos veículos midiáticos, além disso, a divulgação da notícia com o tom em que foi disseminada (no qual, a atriz teria entregado o bebê por um mero capricho), manchou sua honra e imagem, atribuindo-lhe uma imagem negativa perante os olhos da sociedade brasileira. Para além disso, a violação mais óbvia resta não apenas no vazamento da história da atriz em si, mas no vazamento do prontuário do bebê, ato expressamente vedado pelo art. 5º, LXXIX, uma vez que se divulgou um conjunto de dados pessoais (data de nascimento, local, peso, filiação) (BRASIL, 1988).

No ponto de vista do Código Civil de 2002, houve um claro desrespeito nos direitos de personalidade. Conforme ilustra o art. 17 do Código, a exposição do nome da pessoa não pode ser realizada de modo que a exponha ao desprezo público, ainda que sem intenção difamatória (BRASIL, 2002), ou seja, ainda que o ato de exposição da história tenha ocorrido para fins de informar a sociedade, o ato de escolher expor a história atribuindo características negativas a atriz ou à ação de entrega voluntária para a adoção, ensejou o desprezo do público brasileiro, e assim, infringiu-se diretamente o artigo do Código.

Ainda, traçando um paralelo ao art. 5º, X, da Constituição Federal, o art. 21 do Código Civil complementa que a vida privada da pessoa natural é inviolável (BRASIL, 2002). De modo que a divulgação das atividades privadas da atriz vai expressamente ao encontro do referido artigo.

Nesse sentido, a Súmula n.º 403 do Superior Tribunal de Justiça determinou que "independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais". Logo, a divulgação da história da atriz pelos portais midiáticos, buscando o lucro por meio do acesso aos seus sites e perfis, caracteriza-se na hipótese da súmula, garantindo à Klara seu direito indenizatório.

No que tange as legislações específicas de tratamento de dados pessoais no Brasil, é possível afirmar que houve a violação da Lei do Marco Civil da Internet e da LGPD. Apesar da Lei do Marco Civil da Internet possuir apenas um caráter orientador, designando as melhores condutas para o uso da internet e regulando apenas o uso por empresas, a divulgação do caso pelos portais midiáticos vai de encontro com os limites atribuídos pela lei, os quais preveem a vedação a quaisquer atos contra a privacidade e dados pessoais, ainda que os usuários aleguem o uso da liberdade de expressão e comunicação, vide artigos 2º e 3º (BRASIL, 2014).

Dispõe o art. 7º, I, da Lei do Marco Civil da Internet:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 2014)

Pois bem, dessa forma, a Lei corrobora com a proteção ao direito fundamental constitucional de inviolabilidade da intimidade e da vida privada, atribuindo ao autor a capacidade postulatória e ao julgador a capacidade sancionatória de indenização por qualquer dano material ou material decorrente da violação. Dessa forma, afirma-se que, diante da divulgação, houve também a violação da Lei do Marco Civil, nos moldes dos artigos mencionados.

Quanto a LGPD, é possível afirmar que o vazamento de dados gabaritou quase todos os artigos da lei. Primeiramente, violou-se o requisito essencial para o tratamento de dados pessoais (e a única hipótese legal que garantisse a coleta e divulgação das informações): o consentimento, exposto na forma do art. 7º, I, da Lei (BRASIL, 2018). Ora posto, a atriz optou por realizar todos os procedimentos médicos no Hospital Brasil, consentindo com a coleta e tratamento de seus dados apenas para tal, de modo que o vazamento de sua estadia e gravidez revelam um vício de consentimento (art. 8º, 3§, da LGPD), no qual o autor do vazamento utilizou de informações coletadas para outros fins senão aqueles outrora conhecidos pela titular.

Em segundo lugar, violaram-se os princípios da lei: (i) desviou-se da finalidade consentida para o tratamento, (ii) não havia a necessidade legal para a divulgação dos fatos, (iii) não foi informado à atriz que haveria tal divulgação quando a mesma consentiu com a coleta das informações e seus dados não foram tratados com segurança e responsabilidade. Ainda, violaram os fundamentos da lei, quais sejam, as garantias do respeito da privacidade do titular e da inviolabilidade da intimidade, honra e imagem.

Por fim, importante ressaltar que além do vazamento de dados pessoais da atriz, com a atribuição da história ao seu nome, vazaram seus dados pessoais sensíveis, tendo em vista que se divulgou a realização de um procedimento médico, com data, local e justificativa.

No que tange a responsabilidade no vazamento de dados, no caso em tela, é provável que a operadora busque eximir-se da responsabilidade, sustentando que não divulgou os dados e, portanto, detinha controle efetivo sobre o incidente. Contudo, evidencia-se uma falha na prestação do serviço, especialmente no que tange à inobservância do dever de segurança e à proteção dos dados pessoais de seus clientes, bem como das informações de seu sistema interno. O vazamento das informações pessoais viabilizou a conduta lesiva praticada pela profissional de enfermagem, motivo pelo qual o hospital, na qualidade de controlador, deve responder pelos danos causados, uma vez que decorre do risco inerente à sua atividade econômica.

Assim, a LGPD prevê em seu art. 42 (BRASIL, 2018) que o dano extrapatrimonial decorrente da violação da legislação de proteção de dados pessoais é passível de reparação. Isto é, aplica-se a responsabilidade objetiva, uma vez que o dispositivo legal não exige a comprovação de culpa, fundamentando-se na teoria do risco - todo aquele que exerça atividade potencialmente capaz de causar danos a terceiros deve responder por sua reparação, desde que estejam configurados os elementos caracterizadores da responsabilidade civil.

Dita Venosa quanto a capacidade de indenização pela violação de direitos de personalidade ou extrapatrimoniais:

> Diz-se que os direitos da personalidade são extrapatrimoniais porque inadmitem avaliação pecuniária, estando fora do patrimônio econômico. As indenizações que ataques a eles podem motivar, de índole moral, são um substitutivo de um desconforto, mas não se equiparam à remuneração ou à contraprestação. Apenas no sentido metafórico e poético podemos afirmar que esses direitos pertencem ao patrimônio moral de uma pessoa. São irrenunciáveis porque pertencem à própria vida, da qual se projeta a personalidade. (2023, p. 305)

Logo, a indenização pelo dano causado à um direito de personalidade possui apenas uma natureza compensatória para a vítima. Nesse sentido, importante relembrar que no caso concreto em estudo, o Judiciário brasileiro imputou ao responsável a pena pecuniária de R$ 1.000.000,00 (um milhão de reais), sendo reduzida para R$ 200.000.00 (duzentos mil reais) quando reformada pela 1ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo (MIGALHAS, 2024).

A redução da condenação expõe a incapacidade do judiciário em atribuir penas realmente severas para vazamentos de dados, atribuindo-lhes a devida importância.

Em que pese a gravidade dos fatos e a ampla repercussão da notícia, o montante arbitrado revela como a condenação não possui sequer uma natureza indenizatória. Conforme as Demonstrações Financeiras Individuais e Consolidadas da Rede D'OR São Luiz de 2014 (REDE D'OR, p. 17), o conglomerado hospitalar fechou o ano de 2024 com um lucro bruto de R$ 9.462.552.000,00 (nove bilhões, quatrocentos e sessenta e dois milhões, quinhentos e

cinquenta e dois mil reais). De modo que tal condenação corresponde a apenas 0,0021% (zero vírgula zero zero vinte e um por cento) do lucro bruto anual, não chegando ao percentual de 2% (dois por cento) determinado pela LGPD, na forma do art. 52, II (BRASIL, 2018).

Ainda que Venosa compreenda que "a reparação do dano moral deve guiar-se especialmente pela índole dos sofrimentos ou mal-estar de quem os padece, não estando sujeita a padrões predeterminados ou matemáticos" (2023, p. 797), a legislação brasileira já possui um parâmetro a ser observado quando da fixação da condenação em casos de vazamentos de dados, e a inobservância desse implica em uma instabilidade jurídica e descaso para com a temática e a vítima. Com isso, verifica-se que a função reparadora da atribuição da responsabilidade civil deixou de ser imputada corretamente.

Em casos similares de vazamento de dados, o Tribunal de Justiça de São Paulo entendeu:

> DIREITO DO CONSUMIDOR – AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS – "GOLPE DO BOLETO" – RESPONSABILIDADE OBJETIVA DA INSTITUIÇÃO FINANCEIRA – VAZAMENTO DE DADOS SIGILOSOS – SÚMULA 479 DO STJ – DEVER DE RESSARCIMENTO – DANO MORAL CONFIGURADO – RESPONSABILIDADE DO BANCO INTERMEDIÁRIO AFASTADA.
>
> 1. Aplicação do Código de Defesa do Consumidor (CDC), com inversão do ônus da prova em favor da parte autora, nos termos do art. 6º, VIII.
> 2. Consumidora vítima de fraude ao tentar quitar financiamento bancário – criminoso obteve acesso a informações sigilosas do contrato e forneceu boleto falso para pagamento.
> 3. Responsabilidade objetiva da instituição financeira pela falha na segurança dos dados do cliente – risco inerente à atividade bancária – Súmula 479 do STJ.
> 4. Dever do Banco Votorantim de restituir o valor pago indevidamente (R$ 2.500,00) e compensar danos morais (R$ 3.000,00), com correção monetária e juros. No caso, diante do reconhecimento da falha na prestação dos serviços, de rigor a indenização por danos morais. Trata-se de vazamento de dados sigilosos que foram indevidamente acessados por terceiros, gerando transtornos à parte autora e a necessidade de ingresso judicial para reparação do ocorrido. A fixação do valor dos danos morais deve atender aos princípios da proporcionalidade e da razoabilidade. Ressalte-se que a quantia deverá servir de estímulo ao agente a abandonar o comportamento causador do dano, diminuindo, assim, a reiteração de condutas lesivas a direitos de personalidade. Assim, além de promover a efetiva compensação pelo prejuízo suportado, deve-se observar o porte econômico das partes, sobretudo de quem pratica o ilícito. Com isso, a compensação dos danos morais deve ser arbitrada em valor que tenha em conta sua natureza punitiva e compensatória. Aquela, como uma sanção imposta ao ofensor, por meio da diminuição de seu patrimônio, e esta para que a reparação pecuniária traga satisfação mitigadora do dano havido.
> 5. Banco Bradesco, que apenas intermediou o pagamento, não responde pelo evento danoso – inexistência de falha na prestação do serviço.
> 6. Sentença parcialmente procedente – condenação do Banco Votorantim às custas e honorários advocatícios – honorários recíprocos em relação ao Banco Bradesco, observada a gratuidade da justiça.
>
> (TJSP, Processo nº 1001588-65.2021.8.26.0268, Comarca de Itapecerica da Serra, Juíza Ana Rita de Figueiredo Nery, julgado em 20/09/2021).

E o Tribunal de Justiça do Ceará:

> CIVIL. PROCESSUAL CIVIL. APELAÇÃO CÍVEL. CÓDIGO DE DEFESA DO CONSUMIDOR . AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANOS MORAIS E PEDIDO DE TUTELA ANTECIPADA. SENTENÇA PARCIALMENTE PROCEDENTE. UTILIZAÇÃO INDEVIDA DE DADOS PESSOAIS. EXCLUSÃO DOS DADOS DETERMINADA . VIOLAÇÃO AO DIREITO À PRIVACIDADE. LEI GERAL DE PROTEÇÂO DE DADOS (LGPD). DANOS MORAIS CONFIGURADOS. IN RE IPSA . QUANTUM INDENIZATÓRIO. PATAMAR RAZOÁVEL. APELO CONHECIDO E NÃO PROVIDO. ACÓRDÃO Vistos, relatados e discutidos os presentes autos, acordam os membros da Primeira Câmara de Direito Privado do Tribunal de Justiça do Estado do Ceará, à unanimidade de votos, em CONHECER do recurso para NEGAR-LHE PROVIMENTO . Fortaleza, data e hora indicadas no sistema. DESEMBARGADOR FRANCISCO MAURO FERREIRA LIBERATO Relator/Presidente do Órgão Julgador
> (TJ-CE - Apelação Cível: 02549765920228060001, Fortaleza, Relator.: FRANCISCO MAURO FERREIRA LIBERATO, Data de Julgamento: 09/10/2024, 1ª Câmara Direito Privado, Data de Publicação: 09/10/2024)

Ditou o relator, no inteiro teor do acórdão (2024) do caso:

> No caso concreto, restou comprovado nos autos que o hospital utilizou indevidamente os dados pessoais dos apelados (número de telefone e endereço residencial) em receitas médicas distribuídas a terceiros, o que configura violação ao dever de proteção dos dados pessoais. Tal conduta caracteriza-se como ato ilícito, o que justifica a imposição da obrigação de excluir tais dados de seus registros, a fim de cessar a continuidade da violação e prevenir novos transtornos. [...] A questão relativa à indenização por danos morais também deve ser analisada sob a ótica da jurisprudência consolidada desta Corte e do Superior Tribunal de Justiça (STJ), que reconhecem que a exposição indevida de dados pessoais, que resulte em transtornos e invasão à privacidade, ultrapassa o mero aborrecimento cotidiano e enseja reparação por danos morais.

Logo, embora no caso em estudo não se afigure um posicionamento firme do judiciário, já houve um histórico de condenações incisivas no país.

Quanto a responsabilidade dos veículos de notícias responsáveis pela divulgação das informações, embora o art. 43 da LGPD (2018, BRASIL) estabeleça exceção para fins jornalísticos, esta não é absoluta - deve respeitar os limites da atividade legítima e não pode servir de escudo para a divulgação irresponsável de dados obtidos ilicitamente. Além disso, o Marco Civil da Internet reforça essa proteção no art. 7º, garantindo aos usuários o direito à inviolabilidade da intimidade e à indenização por danos decorrentes de sua violação (BRASIL, 2014).

Nesse sentido, traçando um paralelo ao caso em estudo, o Superior Tribunal de Justiça já compreendeu pelo direito à desindexação no âmbito da internet, determinado a retirada de conteúdos ofensivos relativos a dados da vida da parte autora. No *leading case*, tratava-se de uma promotora de justiça, acusada pela mídia de fraude em concursos públicos, o que não restou comprovado.

Ditou o acórdão da Terceira Turma:

> "existem circunstâncias excepcionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais, deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca". Ainda segundo o julgado, "o rompimento do referido vínculo sem a exclusão da notícia compatibiliza também os interesses individual do titular dos dados pessoais e coletivo de acesso à informação, na medida em que viabiliza a localização das notícias àqueles que direcionem sua pesquisa fornecendo argumentos de pesquisa relacionados ao fato noticiado, mas não àqueles que buscam exclusivamente pelos dados pessoais do indivíduo protegido" (STJ, REsp 1.660.168/RJ, 3.ª Turma, Rel. Min. Nancy Andrighi, Rel. p/ Acórdão Min. Marco Aurélio Bellizze, j. 08.05.2018, DJe 05.06.2018).

O direito garantido no acórdão expõe a proteção aos direitos de personalidade da autora. Isto é, ao determinar a retirada das notícias falsas, que vincularam a identidade da autora à tais informações, o STJ atuou preenchendo a lacuna normativa do país, na qual inexistia a previsão legal para a proteção de dados.

Outrora, em que pese a condenação do caso não mencionar a determinação da remoção das notícias da internet, compreende-se como o mínimo para o início da reparação dos danos à autora, tal determinação, uma vez que seu nome segue até os dias atuais vinculados ao caso que tentou manter em sigilo, por todos os meios legais que lhe era assegurado.

Por fim, importante mencionar que além de toda previsão legal de garantia ao sigilo de informações da vida privada pessoal individual, privacidade e não compartilhamento de informações, o STJ também já decidiu acerca da garantia do sigilo judicial quanto a entrega do bebê para adoção pela gestante ou parturiente:

> A gestante ou parturiente que manifeste o interesse de entregar seu filho para adoção tem direito ao sigilo judicial em torno do nascimento e da entrega da criança, inclusive em relação ao suposto genitor e à família ampla. (STJ, 3ª Turma. REsp 2.086.404-MG, Rel. Min. Moura Ribeiro, julgado em 29/09/2024 [Info 835]).

Outrossim, ilustrasse como do caso concreto incorreram diversas violações aos direitos fundamentais, de personalidade e garantidos pela legislação brasileira.

4.2 Análise do Caso Sob a Luz da Legislação Brasileira na Perspectiva Regulatória

Em adição, deve-se estudar o caso em tela à luz das normativas dos órgãos reguladores e autoridades administrativas.

Conforme mencionado, inexiste a menção da intervenção da ANPD no caso, qual seja mediante provocação ou por livre iniciativa. Dessa forma, analisar-se-á as sanções cabíveis se uma vez notificada a responsável para agir.

Logo, embora haja a possibilidade de aplicação de multa, a postura adotada pela autoridade reguladora, conforme se depreende de seus informativos e manuais, revela um viés predominantemente responsivo, com uma natureza orientativa e menos punitiva. *A priori*, se comprovado que houve a comunicação do incidente à autoridade competente, antes que o público ou a Autoridade tivesse ciência, poderá se considerar uma circunstância atenuante, uma vez que evidencia um comportamento pautado pela transparência e pela boa-fé, conforme disposto no inciso II, § 2º, do artigo 52 da LGPD. (BRASIL, 2018)

Uma vez notificada do incidente, a Autoridade verificará a gravidade da situação e poderá, caso entenda necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências específicas, tais como medidas voltadas à reversão ou mitigação dos efeitos do evento danoso - inciso II, § 2º, artigo 48 da LGPD (BRASIL, 2018).

Quanto às sanções aplicáveis, além da multa prevista, existem sanções potencialmente mais gravosas. Destacam-se, nesse contexto, a publicização da infração, após sua devida apuração e confirmação (inciso IV, artigo 52), e a eliminação dos dados pessoais vinculados à infração (inciso VI, artigo 52) (BRASIL, 2018).

Tais penalidades podem, na prática, inviabilizar a continuidade das atividades empresariais. A publicização da infração, além de constituir um juízo técnico da autoridade competente passível de embasar inúmeras demandas judiciais de reparação de danos, poderia impactar negativamente o valor de mercado de empresas de capital aberto, gerando reflexos econômicos significativos e a eliminação dos dados pessoais implicam na perca de informações passíveis de conversão em renda, como a venda de determinadas informações para fins de marketing.

Outrossim, tendo em vista que se trata de um caso de vazamento individual, é possível haver uma conciliação direta entre o controlador e o titular dos dados. Porém, na ausência de acordo, o controlador poderá estar sujeito à aplicação das penalidades cabíveis (§ 7º, artigo 52 da LGPD) (BRASIL, 2018).

Assim, adentra-se ao estudo da quebra do sigilo pela empresa, por meio de uma profissional de enfermagem, conforme apontado pelo relato da atriz. O Código de Ética dos Profissionais de Enfermagem - Resolução n.º 564/2017, por meio do art. 52 (COFEN) veda de forma expressa a divulgação de fatos conhecidos por meio do exercício da profissão, excetuando-se nos casos de consentimento do titular, por previsão legal ou determinação judicial. Contudo, conforme apontado pela atriz, inexistiu nenhuma dessas exceções legais que motivassem o compartilhamento de sua história.

Com o vazamento realizado por um profissional do Hospital Brasil, pertencente ao grupo Rede D'OR São Luiz, a responsabilidade não é apenas do indivíduo, mas também recai sobre a empresa, a qual conforme as normas RN n.º 507/2022 e RN n.º 518/2022, deve garantir boas práticas de gestão organizacional, atuando para garantir uma melhor experiência para o usuário (ANS, 2022). O item 1.5.2 da RN n.º 507/2022 determina que é dever da operadora de saúde a firmação de um termo de confidencialidade, estabelecendo aos seus funcionários o dever de "guardar sigilo e zelar pela privacidade das informações confidenciais a que tiver acesso, sem divulgá-las para pessoas não autorizadas" (ANS, 2022), além disso, conforme o item 1.5.3, as informações coletadas devem ser armazenadas de modo a garantir sua disponibilidade, integridade e confidencialidade, cabendo a empresa a comprovação do preenchimento de todos os requisitos do item.

Sob a ótica da RN n.º 518/22, Anexo III, item 1.3, (ANS) a operadora de saúde deve atuar estabelecendo regras de condutas e de ética, e conforme o item 1.4, deve possuir um programa de integridade e aplicação efetiva de códigos de ética e conduta internas, de modo a atuar prevenindo quaisquer irregularidades.

Em que pese o Hospital não ter se manifestado quanto a adoção de tais medidas, em consulta ao website institucional da operadora é possível visualizar que este, atualmente, possui um Programa de Integridade, contando com um Código de Conduta, uma Política do Programa de Integridade e uma Política de Privacidade (não é possível verificar se o Hospital já contava com tais políticas na época do fato).

Assim, em seu Programa de Integridade a empresa afirma que disponibiliza seu Código de Conduta em seus principais canais e realizam treinamentos "em todas as unidades e áreas significativas da empresa, com o intuito de reforçar a cultura ética e divulgar as ações e projetos desenvolvidos pelo Compliance." (REDE D'OR, p. 7), além disso, se comprometem em "cumprir e fazer cumprir as leis, padrões e regulamentações aplicáveis ao nosso negócio." (REDE D'OR, p. 10).

Já no Código de Conduta da operadora, quanto à proteção de dados pessoais, dita:

> A Companhia, em estrita observância às leis e boas práticas, adota um conjunto de diretrizes éticas e legais quanto ao tratamento de dados pessoais de titularidade de suas Partes Interessadas. Tais diretrizes dão especial atenção ao tratamento de dados pessoais de crianças e adolescentes, bem como a questões específicas aplicáveis ao setor de saúde, como, por exemplo, particularidades envolvendo o tratamento de dados pessoais sensíveis, assim definidos nos termos da legislação aplicável. A Companhia mantém o compromisso de tratar dados pessoais de maneira transparente e segura, a partir da implementação de medidas que garantam a privacidade desde a concepção de produtos e serviços, adotando-as como procedimento padrão. Ademais, a Companhia enfatiza o tratamento de dados pessoais pautado na menor abrangência possível, ou seja, de maneira proporcional e não excessiva, de modo a atender às finalidades determinadas, com estrita observância dos princípios legais e criação de

> mecanismos efetivos para atender de maneira eficaz os direitos dos titulares. Por fim, a Companhia adota medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. A Companhia respeitará a utilização dos nomes sociais de seus pacientes, garantindo registro seguro de dados pessoais em prontuário, conforme diretrizes internas. (REDE D'OR, p.8).

O texto elaborado se apresenta de forma genérica, alegando o compromisso da empresa com o tratamento de dados pessoais, sempre indicando que será realizado conforme a legislação e nos moldes cabíveis ao caso.

Quanto à conduta profissional, o Código de Conduta versa apenas que "a Companhia espera que todos os seus colaboradores se comportem de forma profissional, ética e respeitosa durante a execução das suas atividades cotidianas." (REDE D'OR, p.9). De forma muito interessante, a operadora incluiu um tópico acerca do uso responsável de e-mail, internet e mídia social, contudo, no texto não se visualiza nada acerca da vedação expressa à divulgação de informações internas, de imagens, prontuários ou pacientes:

> E-mails, sistemas e recursos de internet usados no ambiente de trabalho são de propriedade da Companhia e o uso dos mesmos deve ser prioritariamente para propósitos relacionados ao trabalho realizado. O colaborador não deve ter expectativa de privacidade quanto a informações transmitidas ou armazenadas por meio dos sistemas informáticos, e-mail, smartphones ou celulares da Companhia. O uso impróprio ou ilegal destes recursos está sujeito a ações disciplinares. A Companhia se reserva o direito, sujeito à lei aplicável, de acessar e monitorar o uso destes sistemas. Com respeito a aplicativos sociais e rede de mídia social, todos os empregados devem ter em mente que a sua imagem e a imagem da Companhia estão intimamente relacionadas. É importante considerar que mensagens nestes veículos podem potencialmente ser acessadas por clientes, pacientes, parceiros de negócio e acionistas da Companhia. Adicionalmente, o colaborador deve se assegurar de que qualquer informação divulgada ao público não pareça ou cause a impressão de se tratar de posicionamento oficial da Companhia. (REDE D'OR, p.11).

Tal menção ao sigilo das informações vem apenas no tópico de sigilo médico e confidencialidade, o qual estabelece que:

> Todos os colaboradores devem preservar o sigilo médico, a privacidade e a confidencialidade de dados relacionados aos pacientes, incluindo dados pessoais ou qualquer outra informação de caráter privado, confidencial ou proprietário. Os colaboradores da Companhia devem, ainda, manter o sigilo sobre informações confidenciais ou de caráter privado de outros colaboradores e de terceiros com quem a Companhia mantém relacionamento profissional ou de negócios. A divulgação de dados, informações e documentos entre colaboradores ou outras pessoas de fora da Companhia é totalmente proibida, salvo se exigida por lei ou requerida mediante ordem judicial. Qualquer informação, mesmo que relacionada a fato de domínio público, só poderá ser exposta ou divulgada mediante validação e autorização prévias do responsável técnico da unidade assistencial da Companhia. (REDE D'OR, p.12).

Como meio de responsabilização interna, a operadora estabelece que a violação às regras do Código ou das Políticas internas implica nas seguintes sanções disciplinares:

> A. advertência verbal;

> B. advertência escrita;
>
> C. suspensão de até 30 (trinta) dias corridos, quando aplicável;
>
> D. com relação a fornecedores e colaboradores terceiros, notificação ao seu empregador informando o ocorrido e exigindo a sua imediata substituição. Pode haver, ainda, comunicação das condutas potencialmente ilícitas às autoridades para apuração de responsabilidades. (REDE D'OR, p.22).

Importante pontuar que o Código também prevê que a violação de leis culmina em penalidades cíveis e criminais (REDE D'OR, p.22).

Ademais, em análise à Política de Privacidade da operadora, verifica-se que esta segue os padrões da LGPD, informando aos titulares quanto ao Encarregado nomeado (com suas informações de contato), as finalidades para coleta, tratamento, compartilhamento e transferência internacional, armazenamento e meios de segurança de dados. (REDE D'OR, 2025).

Quanto à estrutura de *Compliance* Digital, em análise ao website da operadora, não há como verificar sua existência ou sequer o cumprimento dos requisitos expostos no trabalho, isto é, não foi possível localizar a nomeação de um Comitê responsável pela Proteção de Dados, um documento de mapeamento dos dados internos, um mapa de riscos ou sequer o RIPD.

Logo, apesar da disponibilidade de diversos materiais institucionais, a empresa demonstra uma inobservância às normas da ANS e ANPD, com um *compliance* genérico – o que reflete no incidente ocorrido.

Sob tal avaliação, conclui-se que apesar de dispor de variedade de normas, de observância obrigatória ou não, o Hospital, a enfermeira, os jornalistas e seus jornais, deixaram de seguir tais disposições, incorrendo em diversos danos à direitos amplamente resguardados no país. E para além disso, apesar de todas normativas dispostas, contentou-se o judiciário com uma condenação genérica e ínfima, incorrendo no risco de sequer gerar uma indenização com viés punitivo.

5 CONSIDERAÇÕES FINAIS

O caso Klara Castanho evidencia a necessidade de uma abordagem rigorosa e multidisciplinar para a proteção de dados sensíveis no Brasil, especialmente no setor da saúde.

De modo que, da análise do caso concreto e das normativas de proteção de dados no país, conclui-se que o caso da atriz foi subjugado, uma vez que houve apenas uma mera condenação em danos morais, no âmbito judiciário, ao Hospital responsável, sem qualquer outra penalidade ou orientação definida para os responsáveis (jornalistas, jornais, enfermeira). Além disso, inexistem quaisquer demonstrações de atuação dos órgãos reguladores no caso, de modo a atuarem em uma fronte ampla.

A análise realizada demonstra que a fragilidade na governança da privacidade de informações pessoais e a inobservância de normativas específicas resultam em violações graves aos direitos fundamentais, exigindo medidas corretivas e preventivas mais efetivas.

A violação dos direitos da atriz encontra respaldo no ordenamento jurídico brasileiro, iniciando-se pela garantia constitucional da inviolabilidade da intimidade, vida privada, honra e imagem, na forma do art. 5º, X, da Constituição Federal de 1988 (BRASIL), complementada pelo direito fundamental à proteção de dados pessoais, também no art. 5º, no inciso LXXIX da Carta Magna (BRASIL). Esses dispositivos fundamentais ganham concretude através na LGPD e no Código Civil Brasileiro, os quais estabelecem o regime jurídico específico para o tratamento de dados, com especial rigor para os dados sensíveis relacionados à saúde (art. 5º, II, da LGPD) (BRASIL, 2018) e para a disseminação de informações acerca da vida privada da atriz, expondo-a ao desprezo público (artigos 17 e 21 do Código Civil de 2002) (BRASIL).

A responsabilidade do Hospital Brasil pode ser analisado sob a ótica de diversas vertentes. Como controlador dos dados nos termos do art. 5º, VI da LGPD, o estabelecimento falhou gravemente em seu dever de implementar medidas técnicas e administrativas aptas a proteger os dados pessoais (art. 46), configurando violação dos princípios da finalidade, adequação e necessidade (art. 6º). Essa conduta omissiva gera uma responsabilidade objetiva nos termos do art. 42 da LGPD, independentemente de comprovação de culpa (BRASIL, 2018), e com a responsabilidade, gera o dever de reparação.

Além disso, administrativamente, as sanções administrativas previstas no art. 52 mostram-se plenamente aplicáveis, - ainda que não aplicadas -, desde multas que podem alcançar 2% do faturamento (limitadas a R$ 50 milhões) até a publicização da infração e suspensão das atividades de tratamento de dados, a fim de garantir a ciência de todos os titulares quanto a falha no tratamento de dados pela empresa (art. 52, I, II, IV, da LGPD) (BRASIL, 2018).

No âmbito cível, a violação dos direitos de personalidade (arts. 11 e seguintes do Código Civil de 2002) (BRASIL) justifica ampla reparação por danos morais e materiais, com valor indenizatório que deve considerar tanto o intenso sofrimento causado quanto o caráter pedagógico da punição.

A jurisprudência nacional também reforça o entendimento de que a exposição indevida de informações sensíveis, decorrentes da falha na prestação de serviços, gera dano moral, devendo o responsável pelo dano indenizar ao vitimado.

No que tange à responsabilidade individual da profissional de enfermagem envolvida, esta deve enfrentar consequências éticas e legais específicas. O Código de Ética da Enfermagem (COFEN, 2017) estabelece no art. 52 o dever absoluto de sigilo, cuja violação sujeita a profissional a sanções disciplinares que podem incluir desde censura pública até suspensão do exercício profissional. Paralelamente, a conduta pode configurar o crime de violação de sigilo profissional previsto no art. 154 do Código Penal de 1940 (BRASIL), demonstrando como uma mesma ação pode gerar repercussões em distintas esferas da responsabilização.

Os veículos jornalísticos que disseminaram as informações também podem ser responsabilizados, especialmente quando a divulgação extrapola o interesse público e atenta contra direitos fundamentais, vide Lei do Marco Civil da Internet.

Ademais, a atuação das agências reguladoras, como a ANPD e a ANS, revela-se essencial para fiscalizar o cumprimento das normativas de proteção de dados e aplicar penalidades adequadas.

Cabe à ANPD a aplicação das sanções administrativas previstas na LGPD, podendo inclusive determinar a realização de auditorias, apresentação do Relatório de Impacto à Proteção de Dados e a aplicação das multas supracitadas (art. 5º, XVII) (BRASIL, 2018).

Ademais, à ANS cabe a revogação de certificações e incentivos, para atuar como um mecanismo disciplinar para que instituições hospitalares aprimorem suas práticas de proteção de dados.

Por fim, destaca-se a importância de medidas preventivas para evitar a repetição de situações semelhantes. A implementação do *compliance*, com um Programa de Integridade atuante, com treinamentos periódicos para profissionais de saúde e o desenvolvimento de técnicas de anonimização de dados são estratégias fundamentais para garantir a conformidade com a LGPD e proteger os direitos dos pacientes, impedindo que tais condutas se perpetuem.

Ora posto, o único modo de evitar determinadas condutas é por meio da conscientização e prevenção. Assim, da análise do caso pela plataforma do Hospital e seus documentos disponibilizados, infere-se que o sistema de compliance não é eficaz, utilizando de normas

internas genéricas, sem a devida especificação à personalidade do negócio e sem a comprovação das medidas de adequação às leis nacionais.

Assim, o caso Klara Castanho constitui um marco para a evolução da proteção de dados no Brasil, ressaltando a necessidade de um alinhamento entre legislação, fiscalização e boas práticas institucionais. A efetividade da LGPD depende, sobretudo, de uma mudança cultural que priorize a segurança da informação e o respeito aos direitos fundamentais, reafirmando a centralidade da privacidade e da dignidade humana no ordenamento jurídico nacional.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Relatório de Impacto à Proteção de Dados Pessoais (RIPD).** Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p9. Acesso em: 05 mar. 2025.

ANTONIA FONTENELLE. **Entrevista com Antonia Fontenelle**. YouTube, 2025. Disponível em: https://www.youtube.com/watch?v=e-sCKj_9b5g. Acesso em: 30 mar. 2025.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. **Constituição de 1988**. Brasília, DF: Diário Oficial da União, 1988.

BRASIL. **Decreto nº 11.129, de 11 de julho de 2022**. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Brasília, DF: Diário Oficial da União, 2022.

BRASIL. **Lei nº 12.695, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Diário Oficial da União, 2014.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Diário Oficial da União, 2013.

BRASIL. **Lei nº 13.509, de 22 de novembro de 2017**. Dispõe sobre a adoção e altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.542, de 1º de maio de 1943, e a Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil). Brasília, DF: Diário Oficial da União, 2017.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Diário Oficial da União, 2018.

BRASIL. **Superior Tribunal de Justiça**. Recurso Especial nº 1.660.168/RJ. 3ª Turma. Relatora: Ministra Nancy Andrighi. Relator para Acórdão: Ministro Marco Aurélio Bellizze. Julgado em 08 maio 2018. Publicado no DJe em 05 jun. 2018.

BRASIL. **Superior Tribunal de Justiça**. Recurso Especial nº 2.086.404-MG. 3ª Turma. Relator: Ministro Moura Ribeiro. Julgado em 29 set. 2024. Informativo 835.

CARVALHO, Vinicius Marques; MENDES, Francisco Schertel. **Compliance: concorrência e combate à corrupção**. São Paulo: Trevisan Editora, 2017.

CASTANHO, Klara Forkas Gonçalez. **Carta aberta**. [S. l]. 25 de junho de 2022. Instagram: @klarafgcastanho. Disponível em: <https://www.instagram.com/p/CfPvGDkuii1/?img_index=1.>. Acesso em: 30 de mar. de 2025.

CEARÁ. **Tribunal de Justiça.** 1ª Câmara de Direito Privado. Processo nº XXXXX-59.2022.8.06.0001. Rel. Des. Francisco Mauro Ferreira Liberato, Fortaleza. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-ce/2782154644. Acesso em: 31 mar. 2025.

CHECK POINT. ***Cyberattacks on the healthcare sector***. Disponível em: https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/. Acesso em: 10 de mar. de 2025.

CHECK POINT RESEARCH. ***The State of Cyber Security 2025: Top threats, emerging trends, and CISO recommendations***. 2025. Disponível em: https://www.checkpoint.com/security-report/. Acesso em: 05 de mar. de 2025.

CONSELHO FEDERAL DE ENFERMAGEM (COFEN). **Resolução COFEN nº 311/2007.** Disponível em: http://www.cofen.gov.br. Acesso em: 10 de mar. de 2025.

CONSELHO FEDERAL DE ENFERMAGEM (COFEN). **Resolução nº 564/2017**. Disponível em: https://www.cofen.gov.br/resolucao-cofen-no-5642017/. Acesso em: 10 de mar. de 2025.

CONSELHO FEDERAL DE MEDICINA (CFM). **Código de Ética Médica: Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019**. Brasília: Conselho Federal de Medicina, 2019.

CONSELHO FEDERAL DE MEDICINA (CFM). **Instrução Normativa (IN) nº 03/21**. Disponível em: https://portal.cfm.org.br/noticias/cfm-regulamenta-tratamento-de-dados. Acesso em: 10 de mar. de 2025.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução nº 1.605/2000.** Disponível em: https://www.saude.df.gov.br/documents/37101/0/CFM.pdf/e426a5e2-7143-d957-793b-0185b9018526?t=1660222456231. Acesso em: 10 de mar. de 2025.

CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO. **Nota Oficial**. Coren-SP. São Paulo, 2022. Disponível em: <https://portal.coren-sp.gov.br/noticias/caso-klara-castanho-coren-sp-detalha-sindicancia-e-mantem-se-a-disposicao-da-atriz/. > Acesso em: 10 de mar. de 2025.

CONTROLADORIA-GERAL DO ESTADO DO PARANÁ. **Manual de implementação da LGPD**. Curitiba: CGE/PR, 2021. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf. Acesso em: 05 de mar de 2025.

CUNHA, Blenda Eduarda de Melo; PEREIRA, Esdras Dalmo Pinto; TIMOTEO, Geovana; BARBOSA, João Victor Arruda; et al.. **As dificuldades de implementação da LGPD no Brasil**. Revista Projeto Extensionistas, Pará de Minas, v.1, n. 2, p. 39-47,jul./dez. 2021. Disponível em: https://periodicos.fapam.edu.br/index.php/RPE/article/view/391/249. Acesso em: 05 mar. 2025.

DALLARI, A. B.; MARTINS, A. C. M. S. **Proteção e compartilhamento de dados entre profissionais e estabelecimentos de saúde**. São Paulo: Revista dos Tribunais, 2021.

DATA PROTECTION AUTHORITY. Disponível em: https://iapp.org/resources/article/data-protection-authority/. Acesso em: 19 maio de 2023.

ESTADÃO. **Conselho de Enfermagem arquiva investigação sobre caso Klara Castanho e nega vazamento de informação**. Estadão. São Paulo, 2023. Disponível em: <https://www.estadao.com.br/emais/gente/coren-sp-arquiva-investigacao-sobre-caso-klara-castanho-e-nega-vazamento-de-informacao/.> Acesso em: 10 de mar. de 2025.

ESTADOS UNIDOS DA AMÉRICA. ***A Resource Guide to the FCPA U.S. Foreign Corrupt Practices Act***. *Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission*, 2012. Disponível em: <www.sec.gov/spotlight/fcpa.shtml>. Acesso em: 14 mar. 2025.

FARIAS, Cristiano Chaves; ROSENVALD, Nelson. **Direito civil: teoria geral**. 4. ed. Rio de Janeiro: Lumen Juris, 2006.

FOLHA DE S. PAULO. **Klara Castanho: jornalista que expôs o caso é demitido**. 2022. Disponível em: <https://f5.folha.uol.com.br/celebridades/2022/07/klara-castanho-jornalista-que-expos-o-caso-e-demitido.shtml.> Acesso em: 30 mar. 2025.

GIDDENS, Anthony. **As consequências da modernidade**. Tradução de Raul Fiker. São Paulo: Editora UNESP, 1991.

GLOBOPLAY. [Título do vídeo não especificado]. Disponível em: https://globoplay.globo.com/v/10704497/. Acesso em: 30 mar. 2025.

KELSEN, Hans. **Teoria geral do direito e do Estado.** Tradução: Luís Carlos Borges. 3º edição, São Paulo: Martins Fontes, 2000. Disponível em: https://estudos001.files.wordpress.com/2014/02/hans-kelsen-teoria-geral-do-direito-e-do-estado.pdf. Acesso em: 05 mar. 2025.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 20. ed. São Paulo: Saraiva, 2016.

MINAS GERAIS. **Tribunal de Justiça**. Processo nº XXXXX-47.2024.8.05.0001. Procedimento Comum Cível. Julgado em 27 abr. 2024. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-ba/2845982954/inteiro-teor-2845982958. Acesso em: 31 mar. 2025.

MINISTÉRIO DA SAÚDE. **Resolução Normativa - RN nº 507, de 30 de março de 2022.** Brasília, DF: Diário Oficial da União, 2022.

MINISTÉRIO DA SAÚDE. **Resolução Normativa - RN nº 518, de 29 de abril de 2022.** Brasília, DF: Diário Oficial da União, 2022.

PAUSEIRO, Sérgio Gustavo de Mattos; PAIVA, Marcella da Costa Moreira de. **Compliance e operadoras de planos de assistência à saúde**. In: V Seminário Internacional sobre Direitos Humanos Fundamentais. Anais [...]. João Pessoa: UNIPÊ, 2019.

PECK, Patricia. **Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados)**. São Paulo: Saraiva Educação, 2021.

PORTAL G1. **Conselho de enfermagem vistoria hospital de SP acusado de vazar informações de Klara Castanho.** São Paulo, 2022a. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2022/06/28/conselho-de-enfermagem-vistoria-

hospital-de-sp-acusado-de-vazar-informacoes-de-klara-castanho.ghtml.> Acesso em: 10 de mar. de 2025.

PORTO, Ederson Garin**. Compliance e Governança Corporativa**. Lawboratory Press, 2020.

REDE D'OR SÃO LUIZ. **Aviso de Privacidade**. Disponível em: https://dpo.privacytools.com.br/policy-view/DPO8r0aQk/1/aviso-de-privacidade/pt_BR. Acesso em: 3 abr. 2025.

REDE D'OR SÃO LUIZ. **Central de Resultados**. Disponível em: https://ri.rededorsaoluiz.com.br/informacoes-financeiras/central-de-resultados/. Acesso em: 3 abr. 2025.

REDE D'OR SÃO LUIZ. **Código de Conduta**. Disponível em: https://www.rededorsaoluiz.com.br/sustentabilidade-2023/governanca/programa-de-integridade/index.html. Acesso em: 3 abr. 2025.

REDE D'OR SÃO LUIZ. **Programa de Integridade**. Disponível em: https://www.rededorsaoluiz.com.br/sustentabilidade-2023/governanca/programa-de-integridade/index.html. Acesso em: 3 abr. 2025.

SÃO PAULO. **Tribunal de Justiça**. 16ª Câmara de Direito Privado. Processo nº 1001588-65.2021.8.26.0268, Rel. Ana Rita de Figueiredo Nery, Itapecerica da Serra, 20 set. 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2641137443/inteiro-teor-2641137445. Acesso em: 31 de mar. De 2025.

SENADO FEDERAL. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Senado Notícias, 1 out. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 31 mar. 2025.

TARTUCE, Flávio. **Manual de Direito Civil: volume único**. 12. ed. Rio de Janeiro: Forense, 2022.

THE NOITE. **Leo Dias – The Noite**. YouTube, 2025. Disponível em: https://www.youtube.com/watch?v=8L-aZnhHO7M&t=49s. Acesso em: 30 mar. 2025.

TRANSPARÊNCIA INTERNACIONAL. **Índice de Percepção da Corrupção 2024**. Disponível em: https://transparenciainternacional.org.br/ipc/2024. Acesso em: 16 mar. 2025.

TRIBUNAL REGIONAL DO TRABALHO DA 10ª REGIÃO. **Tutorial de Mapeamento de Riscos.** Disponível em: https://estrategia.trt10.jus.br/plano-de-gestao-de-riscos/item/485-tutorial-de-mapeamento-de-riscos.html. Acesso em: 05 mar 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. EUR-Lex, 2016. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 05 mar. 2025.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. EUR-Lex, 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 05 mar. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**. EUR-Lex, 2018. Disponível em: https://eur-lex.europa.eu/eli/reg/2018/1725/oj. Acesso em: 05 mar. 2025.

UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (GDPR).** 2016. Disponível em:https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html. Acesso em: 5 mar. 2025.

VENOSA, Sílvio de Salvo. **Direito civil: obrigações e responsabilidade civil** / Sílvio de Salvo Venosa. – 23. ed., – Barueri [SP]: Atlas, 2023.

VENOSA, Sílvio de Salvo. **Direito civil: parte geral** / Sílvio de Salvo Venosa. – 23. ed., Barueri [SP]: Atlas, 2023.