UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

ISADORA SÁ URTIGA RÊGO

RESPONSABILIDADE CIVIL DO HOSPITAL POR INVASÃO DE SISTEMAS E BASES DE DADOS SENSÍVEIS NO ATAQUE HACKER

Recife
2024

ISADORA SÁ URTIGA RÊGO

RESPONSABILIDADE CIVIL DO HOSPITAL POR INVASÃO DE SISTEMAS E BASES DE DADOS SENSÍVEIS NO ATAQUE HACKER

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Pernambuco, como requisito para obtenção do título de Mestre em Direito. Área de concentração: 2.2 Transformações das Relações Jurídicas Privada.

Orientador: Prof. Dr. Silvio Romero Beltrão.

Recife

2024

Catalogação na fonte
Bibliotecária Karollyne Ferreira Dantas, CRB-4/2319

R343r Rêgo, Isadora Sá Urtiga.
Responsabilidade Civil do hospital por invasão de sistemas e bases de dados sensíveis no ataque hacker/ Isadora Sá Urtiga Rêgo. -- Recife, 2024.
159 f.

Orientador: Prof. Dr. Silvio Romero Beltrão.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. Centro de Ciências Jurídicas. Programa de Pós-Graduação em Direito, 2024.

Inclui referências.

1. Responsabilidade Civil - Brasil. 2. Proteção de Dados - Brasil. 3. Direito à privacidade. I. Beltrão, Silvio Romero (Orientador). II. Título.

346.81 CDD (22. ed.) UFPE (BSCCJ 2024-22)

ISADORA SÁ URTIGA RÊGO

RESPONSABILIDADE CIVIL DO HOSPITAL POR INVASÃO DE SISTEMAS E BASES DE DADOS SENSÍVEIS NO ATAQUE HACKER

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Pernambuco, como requisito para obtenção do título de Mestre em Direito. Área de concentração: 2.2 Transformações das Relações Jurídicas Privada.

Aprovado em: 23/07/2024.

BANCA EXAMINADORA

_____
Prof. Dr. Silvio Romero Beltrão (Orientador)
Universidade Federal de Pernambuco - UFPE

_____
Profª. Drª. Fabiola Albuquerque Lobo (Examinadora Interna)
Universidade Federal de Pernambuco - UFPE

_____
Prof. Dr. Ivanildo de Figueiredo Andrade de Oliveira Filho (Examinador Interno)
Universidade Federal de Pernambuco - UFPE

_____
Profª. Drª. Maria Antonieta Lynch de Moraes (Examinadora Externa)
Universidade Federal de Pernambuco - UFPE

Dedico este trabalho a todos os que, de alguma maneira, participaram de forma marcante no meu processo evolutivo, seja por meio de lições ou inspirações, posto que contribuíram significativamente para que eu me torne quem sou.

AGRADECIMENTOS

A vontade genuína de criar uma base cognitiva sólida permeou toda a minha formação acadêmica. Sempre tive de modo muito claro os objetivos basilares que gostaria de galgar na minha trajetória. Essa clareza, que esteve tão presente em minha vida, certamente, é proveniente dos desígnios divinos.

Então, não poderia iniciar esse projeto sem agradecer ao mais importante e relevante para a minha trajetória, Deus. Ele que não só me ensinou a sonhar e orientou meus passos, como também me forneceu todos os instrumentos para que pudesse seguir com os meus projetos, quer sejam simples ou extremamente ambiciosos. A Ele dedico toda a minha vida.

Ademais, agradeço com todo o meu coração à família fenomenal que pertenço. Sou extremamente grata por todo o amor, proteção, cuidado, suporte e ensinamentos que tão gentilmente me concederam. Nesse diapasão, gostaria de proferi um agradecimento especial ao meu pai Daniel e à minha mãe Kyslley. Eles que abdicaram de tanto por mim, pela minha formação e pela minha felicidade.

Não tenho ideia do quão árduo foi para os meus pais me criarem, principalmente, enquanto ainda eram adolescentes. Ora, meu pai não apenas precisou abdicar de alguns dos seus projetos para acompanhar o meu crescimento, mas também passou a trabalhar em cidades distintas para manter o sustento da casa. Nunca me esquecerei das suas incontáveis idas a Picos para garantir que pudesse estudar na melhor escola e para que nada me faltasse.

Por outro lado, minha mãe precisou aprender a lidar tanto com os inimagináveis julgamentos de seus pares por ter engravidado muito jovem aos olhos da época, quanto com as diversas dificuldades que passou para realizar a sua formação, enquanto prestava todo suporte e atenção à minha. Sem contar as inúmeras vezes que me levara para a faculdade e para a clínica, de modo que pudesse ter um acompanhamento adequado em todos os meus deveres.

Aprendi com eles a ser forte e a enfrentar as adversidades da vida com garra, buscando sempre dar o meu melhor. Pude ver na prática que o trabalho duro e a oração superam as maiores adversidades.

Agradeço, mais, ao meu companheiro Charles pelo suporte diário e incentivo constante. Certamente, fora crucial para a adequada execução desse projeto. Sou grata, também, às minhas amadas irmãs Clarissa e Sophia, bem como à minha prima irmã, Luiza Urtiga por todo o amor, companheirismo e zelo.

Sendo de relevante menção a minha enorme gratidão não só aos meus avós Maria Bernadete, José Maria, Luiza Lúcia e José Antônio, aos meus primos Giovana, Leonardo e Heitor, mas também às minhas tias Keylla Urtiga e Anna Klicia, bem como aos meus tios Lucas, Levi e Tiago que me propuseram todo o suporte e base valorativa que carrego com muito orgulho e zelo.

Outrossim, minha jornada foi marcada por pessoas incríveis, as quais tenho o prazer de chamar de amigos, sem os quais não seria nem metade do que sou. Em sede de encerramento deste relevante momento, quero ressaltar que minha trajetória não seria a mesma sem os meus ilustres professores, que foram verdadeiros mestres, os quais não só me ensinaram lições que transcendem a simples matéria, como também abriram meus olhos para questões extremamente relevantes na busca dos meus projetos.

Agradeço, de modo especial, ao meu orientador Silvio Romero Beltrão, que fora crucial não apenas para a materialização do presente projeto, como também pela fundamental participação no meu processo de formação profissional.

RESUMO

O presente trabalho monográfico busca contribuir para o estudo a respeito da responsabilidade civil do hospital, enquanto controlador dos dados sensíveis dos pacientes, nos casos de acesso indevido a tais informações. Inicialmente, será explorada a distinção entre vazamento e acesso indevido a dados. Considerando, para tanto que a salvaguarda das prerrogativas constitucionais que tutelam não somente os dados individuais, mas também, de modo mais abrangente, o direito à privacidade, personalidade, autodeterminação informativa e dignidade do indivíduo são essenciais. Partindo desses pressupostos, analisar-se-á o aspecto da falha na prestação do serviço de tutela dos dados e como esta se correlaciona com os pressupostos da responsabilidade civil. Neste ponto, a pesquisa observará a natureza jurídica do defeito e se possui alguma relação com o instituto da culpa. Ademais, cabe ressaltar que o espectro de análise se concentrará na tutela dos dados no meio digital, em especial, observando a figura do prontuário digital e suas implicações positivas e negativas. Traz-se, pois, a lume o teor da Lei Geral de Proteção de Dados, do Código de Defesa do Consumidor e de vasta doutrina sobre a relevância da tutela dos dados sensíveis na vertente relação. Diante do exposto, em prol da proteção das garantias supramencionadas, da função social da atividade em comento, bem como considerando a análise econômica do direito, busca-se observar qual a responsabilidade do hospital nos casos de acesso indevido a dados sensíveis de saúde. Para tanto, pretende-se desenvolver uma pesquisa de cunho bibliográfico, complementada pela análise doutrinária e documental de revistas especializadas e acervos legais, além de consultas a diplomas internacionais e pesquisas sobre mecanismos probatórios práticos.

Palavras-chave: hospital; responsabilidade civil; acesso indevido; dados sensíveis.

ABSTRACT

This monographic work seeks to contribute to the study regarding the hospital's civil liability as controller of patients' sensitive data in cases of improper access to such information. Initially, the distinction between data leakage and improper access to such information will be explored. Considering, to this end, the safeguarding of constitutional prerogatives that protect not only individual data, but also, more broadly, the right to privacy, personality, informational self-determination and dignity of the individual are essential. Based on these assumptions, the aspect of the failure to provide the data protection service will be analyzed and how this correlates with the assumptions of civil liability. At this point, the research will observe the legal nature of the defect and whether it has any relationship with the institution of fault. Furthermore, it is worth highlighting that the spectrum of analysis will focus on the protection of data in the digital environment, in particular, observing the figure of the digital record and its positive and negative implications. It therefore brings to light the content of the General Data Protection Law, the Consumer Protection Code and a vast doctrine on the relevance of the protection of sensitive data in the relationship aspect. In view of the above, in favor of the protection of the aforementioned guarantees, the social function of the activity in question, as well as considering the economic analysis of the law, we seek to observe the hospital's responsibility in cases of improper access to sensitive health data. To this end, the aim is to develop bibliographical research, complemented by doctrinal and documentary analysis of specialized journals and legal collections, in addition to consultations with international diplomas and research into practical evidentiary mechanisms.

Keywords: hospital; Civil Responsability; improper access; sensitive data.

LISTA DE ABREVIATURAS E SIGLAS

a.C.	Antes de Cristo
AC	Apelação Cível
ADIs	Ações Diretas de Inconstitucionalidade
AES	Padrão de Criptografia Avançada
ART	Artigo
CC	Código Civil
CCPA	Lei de Privacidade do Consumidor da Califórnia
CDC	Código de Defesa do Consumidor
CF	Constituição da República Federativa do Brasil
CFM	Conselho Federal de Medicina
CIDH	Comissão Interamericana de Direitos Humanos
CLT	Consolidação das Leis Trabalhistas
COVID-19	*Corona Vírus Disease* 2019
CP	Código Penal
CPC	Código de Processo Civil
CPF	Cadastro de Pessoa Física
CPP	Código de Processo Penal
FGTS	Fundo de Garantia por Tempo de Serviço
GDPR	Regulamento Geral de Proteção de Dados
HIV	*Human Immunodeficiency Virus*
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IGESDF	Instituto de Gestão Estratégica de Saúde do Distrito Federal
INCA	Instituto Nacional do Câncer
LGPD	Lei Geral de Proteção de Dados
LIA	Lei de Acesso à Informação
PEP	Prontuário Eletrônico do Paciente
PEP	Prontuário Eletrônico do Paciente
REsp	Recurso Especial
RG	Registro Geral
RJ	Rio de Janeiro

RO	Rondônia
S.A	Sociedade Anônima
S/MIME	*Secure/Multipurpose Internet Mail Extensions*
SBIS	Sociedade Brasileira de Informática em Saúde
SP	São Paulo
S-RES	Sistema de Registro Eletrônico de Saúde
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TI	tecnologia da informação
TJ-PR	Tribunal de justiça do Estado do Paraná
TJ-SP	Tribunal de Justiça do Estado de São Paulo
TLS	*Transport Layer Security*
TRCT	Termo de Rescisão do Contrato de Trabalho
TRT-4	Tribunal Regional do Trabalho da 4ª Região
TST	Tribunal Superior do Trabalho
USP	Universidade de São Paulo

SUMÁRIO

1 INTRODUÇÃO

A busca por uma adequada tutela dos dados pessoais vem ganhando contornos significativos na era da tecnologia. A implantação de novos dispositivos, especialmente aqueles que usam redes sem fio e sensores para coletar, armazenar e trocar informações, proporcionou um incremento significativo dos riscos associados ao tratamento das informações pessoais. Estas que, por sua vez, atuam como fatores vitais para as engrenagens da economia da informação.

Os dados em questão estão cada vez mais visados, inclusive, atraindo a atenção de setores mal intencionados. Os quais, por meio de artifícios ardilosos, buscam vantagens indevidas com a quebra da segurança de sistemas e conseguinte acesso indevido a banco de dados.

Nesse contexto, evidencia-se uma atenção considerável da doutrina e jurisprudência quanto a necessidade de analisar as estratégias e regulamentações para nortear uma adequada proteção dos dados pessoais. Contudo, com o significativo aumento dos casos de violação virtual a dados, faz-se necessário um aprofundamento voltado, também, para as remediações e distribuições de responsabilidades, com o fito de materializar uma adequada tutela à esfera jurídica da vítima.

Assim, a presente dissertação surge com o intuito de contribuir para o estudo a respeito da responsabilidade civil por acesso indevido a informações pessoais. Cabendo a realização de um recorte temático quanto a violação a dados médico-hospitalares dos pacientes atendidos na rede privada de saúde em decorrência de invasões a sistemas e bases de dados, popularmente conhecidas como ataques *hacker*.

No Brasil, tais ataques a sistemas de saúde tornam-se cada vez mais expressivos e frequentes[1]. Globalmente, a área médico-hospitalar e a assistência social continuam sendo os setores com o maior número de casos de violação. Especialmente, em decorrência da relevância dos dados tratados.

Ora, hospitais e organizações de saúde já eram alvos atraentes mesmo antes da adoção massiva de protocolos de armazenamento de dados virtuais. Os registros dos

[1]CRYPTOID. **Relatório do Cenário de Ameaças da Tenable: Brasil é o país com o maior volume e dados expostos no mundo.** Disponível em: https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/relatorio-do-cenario-de-ameacas-da-tenable-brasil-e-o-pais-com-o-maior-volume-e-dados-expostos-no-mundo/. Acesso em: 08 jan. 2024.

pacientes têm quase tudo que um invasor precisa em um único documento para realizar esquemas sofisticados de fraude em seguros, comprar suprimentos médicos ou mesmo cometer outros tipos de fraude. O que inclui até mesmo o roubo de identidade total do titular do dado violado. Os registros médicos, portanto, são alvos lucrativos e ativos caros no mercado negro.

Outrossim, a implantação de novos dispositivos tecnológicos é uma faca de dois gumes. Embora esses artifícios ofereçam aos ambientes médicos recursos inovadores para o cuidado com os pacientes e aumentem a eficiência do atendimento, tais dispositivos incrementam a superfície de ataque de uma organização.

Levando em consideração o outrora exposto, surge um relatório da Tenable Research[2] sobre o ecossistema de *ransomware*, um tipo de *software* malicioso que atua criptografando dados e exigindo contraprestações financeiras para libera-los. O supramencionado relatório pontuou quanto a descoberta de uma rede multimilionária impulsionada por dupla extorsão e modelos de *ransomware* como serviço. O qual passou a ser considerado uma verdadeira *commodity* do crime.

Nesse diapasão, parece evidente que as protetivas inerentes à tutela de dados sensíveis correm riscos consideráveis nas relações mediadas pela tecnologia em geral. Inclusive, não se pode falar ainda em confiabilidade absoluta, em rede, na preservação de dados pessoais, mesmo considerando a exigência crescente de aplicação das melhores técnicas de segurança.

Com base no cenário exposto, inicialmente, a presente pesquisa buscará uma compreensão quanto às estruturas jurídicas que permeiam a proteção de dados pessoais, em especial, de cunho sensível de saúde. Essa análise encontra-se estruturada no primeiro capítulo da pressente dissertação.

Considerando, para tanto, a salvaguarda das prerrogativas constitucionais que tutelam não somente os dados individuais, mas também, de modo mais abrangente, o direito à privacidade, personalidade, autodeterminação informativa, sigilo médico e dignidade do indivíduo, as quais são essenciais para um Estado Democrático de Direito.

---

[2] CRYPTOID. **Relatório do Cenário de Ameaças da Tenable: Brasil é o país com o maior volume e dados expostos no mundo**. Disponível em: https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/relatorio-do-cenario-de-ameacas-da-tenable-brasil-e-o-pais-com-o-maior-volume-e-dados-expostos-no-mundo/. Acesso em: 08 jan. 2024.

Partindo desses pressupostos, analisar-se-á o aspecto da falha na prestação do serviço de tutela dos dados e como esta se correlaciona com os elementos da responsabilidade civil. Utilizando como parâmetro não apenas as disposições normativas, mas também questões técnicas inerentes à segurança dos dados e demais deveres inerentes à boa prática hospitalar, isto em sede de encerramento do capítulo inicial.

Ademais, cabe ressaltar que o espectro de análise se concentrará na tutela dos dados no meio digital, em especial, observando a figura do prontuário digital e suas implicações positivas e riscos acrescidos pelo armazenamento em meio digital.

No segundo capítulo, tem-se um dinâmico aprofundamento quanto à responsabilidade civil do hospital, perpassando, inclusive, por contundentes debates quanto a responsabilização do controlador de dados nos casos de ataque hacker. Dispondo, para tanto, quanto aos elementos intrínsecos ao processo de reparação no âmbito cível. Trazendo, mais, a lume o teor da Lei Geral de Proteção de Dados, do Código de Defesa do Consumidor e de vasta doutrina sobre as abordagens realizadas.

Por fim, no terceiro capítulo é explorada a distinção entre vazamento e acesso indevido a dados, bem como os contornos jurídicos inerentes à essa distinção. Delineando, mais, quanto a noção jurídica do dano por acesso indevido a dados sensíveis, considerando os aspectos materiais e morais.

Diante do exposto, em prol da proteção das garantias supramencionadas, da função social da atividade em comento, bem como considerando a análise econômica do direito, busca-se observar qual a responsabilidade do hospital nos casos de acesso indevido a dados sensíveis de saúde. Para tanto, pretende-se desenvolver uma pesquisa de cunho bibliográfico, complementada pela análise doutrinária e documental de revistas especializadas e acervos legais, além de consultas a diplomas internacionais e pesquisas sobre mecanismos probatórios práticos.

2 PREMISSAS NECESSÁRIAS PARA A ABORDAGEM DO TEMA

Em linhas introdutórias, visando um adequado aprofundamento do tema, cabe a análise de algumas estruturas jurídicas que permeiam a proteção de dados pessoais, em especial os de cunho sensível de saúde. Essa compreensão parece imprescindível para a real noção quanto a relevância da temática em tela.

Observar-se-ão, para tanto, algumas noções como o direito à privacidade, à proteção da personalidade, à autodeterminação informativa e à dignidade do indivíduo. Tendo como ponto de partida a adequada compreensão quanto a conceito de dados pessoais sensíveis.

2.1 A RELEVÂNCIA DA PROTEÇÃO DOS DADOS SENSÍVEIS DE SAÚDE

2.1.1 Conceito de dados sensíveis em saúde

A delimitação dos chamados dados pessoais é extremamente relevante para que se aperfeiçoe a protetiva sob análise, na medida em que se estabelecem os limites da própria tutela jurídica. Assim, para o art. 5º da Lei Geral de Proteção de Dados (LGPD)[3], os dados pessoais são informações relacionadas a pessoa natural identificada ou identificável, os quais, segundo dimensiona Bruno Bioni[4], compõe os atributos e características que tornam o indivíduo singular, o chamado prolongamento pessoal.

Para uma análise minuciosa dessa estrutura, o autor propõe, inicialmente, o estabelecimento de uma correlação entre a ideia de singularidade e o ser social, posto que a identificação da identidade do indivíduo ocorre no meio coletivo. Embasando-se, por exemplo, na doutrina traçada por Diogo Costa Gonçalves[5], segundo a qual a pessoa se concretiza quando se relaciona, de modo que ela responde ou procura afirmar-se em meio à comunidade.

Assim, vislumbra-se que a proteção proposta pela normativa sob análise buscou ser bastante abrangente, especialmente quando estabelece um conceito tão amplo sobre dado

---

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

[4] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 59.

[5] GONÇALVES, Diogo Costa. **Pessoa e direitos da personalidade: fundamentação ontológica**. Coimbra: Almedina, 2008, p. 40-60.

pessoal. Evidenciando uma contundente relevância neste *modus operandi*, já que mesmo em um cenário introdutório o dado não se mostre relevante, por meio de um processo de tratamento, no qual algumas informações são cruzadas e organizadas, podem ser formados dados específicos sobre determinada pessoa[6].

O que, considerando um cenário social, no qual o indivíduo se projeta e constrói neste a sua auto delimitação, urge-se a estruturação de uma tutela cada vez mais contundente para que o indivíduo possa ter autonomia ao se relacionar socialmente. Já que proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade, sem discriminação de qualquer natureza, conforme orienta a própria constituição[7].

Dentro das disposições concernentes aos dados em geral encontram-se os denominados dados sensíveis, os quais compreendem uma tipologia distinta em decorrência da natureza do seu conteúdo oferecer uma especial vulnerabilidade. Dentre estes, existem os que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surgindo, dessa forma, a razoável preocupação em haver discriminação ou diferenciação de uma pessoa em detrimento de tais aspectos da sua personalidade.

Bioni[8] chama atenção para uma vertente preocupante do tratamento de dados, na qual uma informação tida como irrelevante pode converter-se em um dado sensível. Esse fenômeno ocorre, particularmente, quando “se têm disponíveis tecnologias que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos”. Assim, entende existir a possibilidade de identificar individualidades mais sensíveis das pessoas a partir de informações triviais[9].

Esse preocupante fenômeno pôde ser observado em um estudo da Universidade de Cambridge[10], no qual observou-se que as “curtidas” em uma rede social poderiam criar um retrato fiel dos gostos e preferências dos usuários. A análise realizada identificou

---

[6] BIONI, *op. cit.,* p. 59.
[7] VIOLA, Marcelo; TEFFÉ, Carolina. Tratamento De Dados Pessoais Na LGPD: Estudo Sobre as Bases Legais Dos Artigos 7.º E 11. *In:* DONEDA, D. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 6, p. 131.
[8] BIONI, *op. cit.*, p. 67.
[9] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. **Private traits and attributes are predictable from digital records of human behavior**. 2013. Disponível em: http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html. Acesso em: 15 nov. 2023.
[10] BIONI, *op. cit.,* p. 67.

características eminentemente intimas dos indivíduos, como a porcentagem dos usuários homossexuais e heterossexuais, os usuários brancos e negros e, por fim, quais teriam uma ligação partidária republicana ou democrata.

Tendo em vista o exposto, a tutela dos mencionados dados pessoais possui tamanha relevância. Ora, esta encontra-se diretamente vinculada a garantias constitucionais de fundamental resguardo. Haja vista que seu uso indevido pode incorrer no desrespeito de protetivas básicas, gerando, por exemplo, diversas modalidades de discriminações, as quais ferem princípios constitucionais basilares.

Nesse contexto, Celina Bodin e Chiara de Teffé[11] evidenciam a possibilidade da ocorrência de graves discriminações, especialmente quando entidades privadas e governamentais se tornam capazes de “rotular” e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos.

Esse cenário pode refletir em problemas evidentemente concretos, como o exemplo trazido pelas autoras, no qual alguns bancos, ao descobrirem que o indivíduo teve um derrame, começam a cobrar o pagamento dos empréstimos realizados[12].

Ressalta-se, também, um dos casos que motivou a edição da Súmula 443 do Tribunal Superior do Trabalho, TST, segundo a qual “presume-se discriminatória a despedida de empregado portador do vírus HIV ou de outra doença grave que suscite estigma ou preconceito. Inválido o ato, o empregado tem direito à reintegração no emprego”[13]. No qual, ao avaliar o acervo probatório constante dos autos, o juiz entendeu que “há subsunção dos fatos à hipótese da dispensa discriminatória, uma vez que a dispensa ocorreu poucos dias após a comunicação pelo obreiro de sua condição soropositiva”[14].

---

[11] MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. **Redes sociais virtuais, privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet**. Revista Pensar, v. 21, n. 1 2017.

[12] INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Transparência e Governança nos algoritmos, um estudo de caso sobre o setor de birôs de crédito.** Rio de Janeiro: ITS, 2017. Disponível em https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf. Acesso em: 15 nov. 2023.

[13] BRASIL. Tribunal Superior do Trabalho. **Súmula nº 443.** Presunção de dispensa discriminatória. Diário da Justiça [da] República Federativa do Brasil. Disponível em: https://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_401_450.html. Acesso em: 29 maio 2024.

[14] TRIBUNAL REGIONAL DO TRABALHO (3ª Região). **Trabalhador dispensado de forma discriminatória após ser diagnosticado com HIV será reintegrado**. Minas Gerais, 19 out. 2021. Seção de Imprensa. Disponível em: https://portal.trt3.jus.br/internet/conheca-o-trt/comunicacao/noticias-juridicas/trabalhador-dispensado-de-forma-discriminatoria-apos-ser-diagnosticado-com-hiv-sera-reintegrado. Acesso em: 15 nov. 2023.

Desse modo, para além das questões práticas outrora mencionadas, outros problemas de ordem grave surgem com o vazamento de determinadas informações sensíveis. Exemplo evidencia-se com a própria questão da estigmatização mencionada na súmula supramencionada.

Para Erving Goffman, *"la sociedade estabelece los médios para caracterizar a las personas y el complemento de atributos, que se perciben como corrientes y naturales a los membros de cada uma de essas categorias"*[15]. Nesse cenário, o conceito de estigma ganha significado relacional na obra do sociólogo canadense, posto que conecta atributos e estereótipos a formas de estigmatização. Assim, o autor analisa como eles são criados e manipulados, e quais os seus efeitos nas interações sociais.

O termo "estigma" proveniente do grego antigo "*stígmata*", o qual fazia referência a uma marca ou cicatriz feita no corpo, passou, no contexto sociológico e psicológico contemporâneo, a referir-se a uma marca, característica ou reputação que causa uma visão negativa a determinada pessoa ou grupo. Refere-se, pois, a preconceitos, desaprovações ou discriminações embasadas em características, comportamentos ou identidades que são tidas por indesejáveis.

A análise sobre o dano causado por um processo de estigmatização será posteriormente realizada. Por ora, urge mencionar que dentre os diversos mecanismo da sua ocorrência, observa-se o fenômeno da criação de um estereótipo que posteriormente é destacado do grupo social, sendo colocado em uma categoria diferenciada. Proporcionando um tratamento diferenciado e injusto, o qual corrobora com o afastamento desse indivíduo de atividades e oportunidades[16].

Em complementação, Caitlin Mulholland[17] dispõe sobre exemplos dados por Cohen[18], a qual relata algumas formas de tratamento inadequado de dados sensíveis que geram discriminação e segregação abusiva no âmbito das relações de consumo. Segundo

---

[15] GOFFMAN, Erving. **Estigma: la identidade deteriorada**. 5.ed. Buenos Aires: Amorrortu Editores, 1993. p. 11.

[16] CRUZ, Natalia. Estigma Social**:** O Que é, Significado e Estigmatização. **Quero Bolsa**, 2022. Disponível em: https://querobolsa.com.br/enem/sociologia/estigma-social. Acesso em: 15 nov. 2023.

[17] MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *In:* MARTINS, G. M.; ROSENVALD, N. (Org.). **Responsabilidade civil e novas tecnologias**. 1ed. Belo Horizonte: Editora Foco, 2020, v. 1, p. 109-124. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 15 nov. 2023.

[18] COHEN, Julie. Examined Lives, Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, p. 1373-1438, 2000. p. 27.

a autora[19] os dados dos consumidores podem ser utilizados para muitos fins com os quais os titulares podem não concordar tão alegremente. Exemplos evidenciam-se nos casos de decisões de emprego e classificações por prestadores de seguros de saúde que excluem ou prejudicam os titulares dos dados, ou questões empregatícias e habitacionais baseadas em riscos de personalidade percebidos ou em preferências sexuais ou religiosas.

Conforme sugere Bioni[20], uma tutela jurídica dos dados sensíveis busca assegurar que o titular das informações possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto, garantindo que o indivíduo "se realize e se relacione na sociedade, o que é um traço marcante dos direitos da personalidade".

Partindo das disposições supramencionadas, evidencia-se que a proteção de dados pessoais está intimamente vinculada com a própria liberdade, pincipalmente no que concerne ao processo de autodeterminação informativa. Ora, tal disposição justifica-se com a percepção de que tais dados projetam a maneira como cada indivíduo é visto na sociedade, o que interfere no próprio exercício de direitos e da cidadania.

Assim, tutelar essas estruturas possibilita a salvaguarda da segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado, assegurando a necessária confiança entre todos os atores desse ecossistema "para que não haja paralisia nessas trocas econômicas"[21].

Outrossim, o Kachani[22] dimensiona que os dados pessoais são o petróleo, insumo ou uma *commodity* para a economia da informação[23]. Acrescentando que há uma verdadeira transformação das pessoas em mercadorias. Inclusive, a economia e a

---

19 Consumer data can be used for many purposes to which consumers might not so blithely agree, employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical "have-nots"; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences.

20 BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 70.

21 *Ibid.,* p. 70.

22 KACHANI, Morris. Ou a sociedade acompanha internet ou a democracia começa a ficar em xeque. **Folha de São Paulo**. 2014. Disponível em: http://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/. Acesso em: 26 jun. 2021.

23 A economia em um modo geral é baseada pelo elemento principal de cada revolução industrial que vivemos ao longo da história. Enquanto o que movia as indústrias na Primeira Revolução Industrial era o vapor e o carvão, na Segunda Revolução Industrial foi a vez do petróleo e da energia elétrica, o que aumentou ainda mais a capacidade industrial dessa era. Atualmente, estamos vivenciando a quarta revolução industrial. Assim, dizer que os dados pessoais são o petróleo, insumo ou uma commodity para a economia da informação, representa associa-los ao principal elemento do momento revolucionário ao qual nos encontramos. Não é por acaso que as principais empresas do mercado hoje em dia estão ligadas diretamente ao ramo dos dados ou tecnologia.

sociedade estão cada vez mais dependentes desse livre fluxo informativo. Fazendo parte da doutrina tratar essa questão como sendo a morte da privacidade ou erosão da intimidade[24].

2.1.2 A proteção de dados na esfera constitucional e o princípio da dignidade da pessoa humana

A necessidade de uma efetiva tutela dos dados, já introduzida anteriormente, ganha contornos ainda mais significativos na sociedade altamente conectada. A facilidade e a velocidade de acesso aos dados pessoais potencializam as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social[25].

Até março de 2022, a Carta Magna dispunha de alguns mecanismos que orientavam uma interpretação no sentido da existência de uma tutela indireta dos dados em questão. Exemplos evidenciam-se com o art. 5º da Constituição, o qual trata sobre diversos direitos e deveres individuais e coletivos, dentre os quais: o sigilo das comunicações de dados[26], a ação de *habeas data*[27] e a inviolabilidade[28] da intimidade, da vida privada, da honra e da imagem das pessoas, inclusive, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Contudo, evidencia-se que o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida[29]. Enquanto que o *habeas data* seria um instrumento com o escopo específico de assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo[30].

---

[24] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 71.
[25] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental À Proteção De Dados. *In:* DONEDA, D. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 2, p. 40.
[26] BRASIL. **Constituição (1988).** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 maio 2024.
[27] *Ibid.*
[28] *Ibid.*
[29] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[30] BRASIL. **Constituição (1988).** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 maio 2024.

Nesse sentido, mesmo diante das considerações supramencionadas, Ingo Wolfgang Sarlet já alertava para a existência de um direito à proteção de dados pessoais como direito fundamental implícito na constituição federal[31], tese esta que era endossada pelo Supremo Tribunal Federal por meio das Ações Diretas de Inconstitucionalidade (ADIs) n. 6387[32], 6388[33], 6389[34] e 6390[35].

Em vista a importância do tema, o constituinte derivado optou por incluir a proteção de dados de modo explícito na Carta Magna, aumentando sua proteção jurídica e esvaindo qualquer debate a respeito do seu reconhecimento ou não como direito fundamental. Surge, pois, a Emenda Constitucional 115 acresceu o inciso LXXIX ao artigo 5º da CF, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"[36].

A positivação da proteção dos dados pessoais passou a conferir a esse direito o status de cláusula pétrea, conforme artigo 60, §4º, IV da CRFB/88[37], impedindo que se tramite no Legislativo proposta de emenda tendente a suprimir ou reduzir a proteção constitucional conferida a esse direito. Ademais, qualquer norma infralegal que contrarie essa proteção será materialmente inconstitucional, o que evidencia, contundentemente, a relevância desse direito.

Para além do exposto, permite-se extrair a fundamentalidade da proteção em análise a partir da interpretação de princípios e direitos fundamentais de caráter geral e especial já positivados. A exemplo do princípio da dignidade da pessoa humana e do direito ao livre e completo desenvolvimento da personalidade.

---

[31] SARLET, I. W. Fundamentos Constitucionais: O Direito Fundamental À Proteção De Dados. *In:* DONEDA, D. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 2, p. 53.
[32] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6387.** Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 29 maio 2024.
[33] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6388**. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357772. Acesso em: 29 maio 2024.
[34] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6389**. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1. Acesso em: 29 maio 2024.
[35] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6390**. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1.Acesso em: 29 maio 2024.
[36] BRASIL. **Emenda Constitucional nº 115, de 15 de dezembro de 2022**. Altera os arts. 21, 40, 201, 203 e 204 da Constituição Federal para dispor sobre o novo regime de previdência complementar dos servidores públicos. Diário Oficial da União: seção 1, Brasília, DF, 16 dez. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=Emenda%20Constitucional%20n%C2%BA%20115&text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais. Acesso em: 29 maio 2024.
[37] BRASIL. **Constituição (1988).** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 maio 2024.

Robert Alexy[38], em sua obra Teoria de los Derechos Fundamentales, faz uma análise distinguindo princípios e regras. O autor destaca que princípio equivale a uma norma a qual determina que algo seja concretizado na maior medida possível, estando dentro das possibilidades jurídicas e fáticas existentes. Para Alexy, os princípios dizem respeito a mandados de otimização, quer seja de permissão como de proibição. Tal distinção entre regras e princípios fica mais evidente frente a busca por um meio de solução do conflito de princípios e do conflito de regras.

Nesse contexto, é importante destacar o entendimento de Flademir Martins[39], segundo o qual havendo a colisão de princípios, um princípio cede, no caso concreto, ante o outro, gerando o que chama de relação de procedência condicionada. Contudo, isso não gera a invalidação do princípio afastado ou a formação de uma cláusula de exceção. Diferente das regras, cuja colisão só pode ser solucionada com a invalidade de uma regra ou com a introdução de uma cláusula de exceção.

Depois dessa breve análise introdutória a respeito de regras e princípios, tem-se um exame específico sobre o princípio da dignidade da pessoa humana. Recordando a história do pensamento ocidental sobre *dignus* , é perceptível que a dignidade da pessoa humana, em um primeiro momento, assume um papel de valor, tido enquanto dimensão interna. Frisa-se que esse conceito está relacionado à conduta correta, à moralidade e ao bem. Já em um momento seguinte, a dignidade da pessoa humana adquire a função de objetivo máximo, dimensão externa, que deve ser atingido pela sociedade e pelo Estado[40].

Nesse cenário, é importante evidenciar a relevância da *dignus* na concretização dos Direitos Humanos. Como destaca Casado Filho[41], a Declaração Universal dos Direitos Humanos de 1948, mais precisamente em seu preâmbulo, já havia empregado o princípio como fundamento da justiça, da liberdade e da paz. Aliado a isso, observa-se[42] que a harmonia entre esses princípios e o valor humano concede coesão, unidade e

---

[38] ALEXY, Robert. **Teoría de los Derechos Fundamentales**. Madrid: Centro de Estúdios Políticos y Constitucionales, 2002.
[39] MARTINS, Flávio José Barbosa. **Dignidade da pessoa humana – princípio constitucional fundamental**. Curitiba: Juruá, 2003, p. 102-103.
[40] BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo – a construção de um conceito jurídico à luz da jurisprudência mundial**. Belo Horizonte: Fórum, 2014, p. 62.
[41] CASADO FILHO, Napoleão. **Direitos humanos fundamentais**. São Paulo: Saraiva, 2012.
[42] MARTINS, Flávio José Barbosa. **Dignidade da pessoa humana – princípio constitucional fundamental**. Curitiba: Juruá, 2003, p. 104.

inelegibilidade aos direitos fundamentais, o que acaba tornando possível um sentido e um alcance nessa relação interpretativa.

O princípio em questão “refere-se aos direitos chamados de primeira geração. Trata-se da dignidade do ser humano, sujeito de direitos, titular por natureza de racionalidade e anseio de liberdade”[43]. Tem-se que a positivação do princípio da dignidade da pessoa humana é, de certa forma, recente, já que, o valor humano passou a ser reconhecido nas Constituições Republicanas somente no decorrer do século XX[44].

Conforme evidencia Maurício Godinho Delgado[45], a dignidade da pessoa humana constitui o fundamento, objetivo e princípio do Brasil. Dessa maneira, representa o primordial valor em que é construída a sociedade brasileira, estando presente, consequentemente, em todos os ramos do Direito e realizando influência nas condutas humanas particulares. Depreende-se, com base nisso, que, tanto o legislador quanto o intérprete da lei, devem sempre procurar a efetivação do princípio da dignidade da pessoa humana.

Ainda de acordo com Martins, tem-se que, nos dias atuais, os princípios consistem em normas vinculantes que detêm plena juridicidade. Dessa maneira, o embasamento da dignidade da pessoa humana está centrado no ser humano.

Nessa conjuntura, é necessário trazer o entendimento de Vicente Paulo e Marcelo Alexandrino[46], o qual afirma que a dignidade da pessoa humana se assenta no reconhecimento de duas posições jurídicas ao indivíduo. Por um lado, apresenta-se como “um direito de proteção individual, não só em relação ao Estado, mas, também, frente aos demais indivíduos. De outro, constitui dever fundamental de tratamento igualitário dos próprios semelhantes”.

Conforme destaca Barroso[47], para chegar ao conceito de dignidade da pessoa humana, é essencial abandonar a ideia de uma apreciação baseada na religiosidade ou

---

[43] ZISMAN, Carlos Roberto. A dignidade da pessoa humana como princípio universal. **Revista de Direito Constitucional e Internacional**. Vol. 96, jul. 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDConsInter_n.96.06.PDF. Acesso em: 26 jun. 2021.

[44] SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2001, p. 63.

[45] DELGADO, Maurício Godinho. **Curso de Direito do Trabalho**. 4. ed. São Paulo: LTr, 2005.

[46] ALEXANDRINO, Marcelo; PAULO, Vicente. **Direito Constitucional Descomplicado**. 16. ed. rev., atual. e ampl. - Rio de Janeiro: Forense. São Paulo: MÉTODO, 2017, p. 90.

[47] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo**. 5. ed. São Paulo: Saraiva, 2015.

ideologia. Consequentemente, a característica dela precisa estar pertinente com a laicidade, isto é, não sendo possível que esteja voltada somente para uma determinada religião, devendo atender a todas as pessoas, independente da religião que elas possuam. Para o estudioso, também é necessária uma neutralidade política, assim sendo, a dignidade da pessoa humana precisa ser dividida entre todos da sociedade, sem diferenciação em relação ao sistema político-econômico de cada um, além de ser universal, ou seja, devendo ser utilizada por todos, sem qualquer tipo de distinção.

Para Ingo Wolfgang Sarlet[48], o conceito de dignidade da pessoa humana é:

> A qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da Comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos.

Dessa maneira, o princípio da dignidade da pessoa humana possui ligação com um grupo de direitos, como, por exemplo, a educação, a paz e a moradia. Em outras palavras, esse princípio equivale a um ajuntamento de todos os direitos fundamentais que existem, com o intuito de que toda a população tenha um tratamento igualitário na sua vida cotidiana[49].

Portanto, é possível concluir que a dignidade consiste em uma característica inerente e distintiva de cada pessoa que faz dela digna de apreço e consideração por parte da sociedade e do Estado, gerando, dessa forma, uma complexidade de direitos e deveres fundamentais que garantem ao ser humano proteção contra atos desumanos e degradantes. Além disso, busca permitir condições mínimas de existência para proporcionar uma vida saudável, com sua atuação nos caminhos da sua própria existência e da vida em cooperação com os outros seres humanos.

As conexões entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção dos dados pessoais são intensas. Conforme dispõe Sarlet [50], os

---

[48] SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2001, p. 60.

[49] JORGE NETO, Francisco Ferreira; CAVALCANTE, José de Queiroz Pereira. **Direito do Trabalho**. 7. ed. São Paulo: Atlas, 2013, p. 105.

[50] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental À Proteção De Dados. *In:* DONEDA, D. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 2, p. 49.

dois principais pontos de contato são o princípio da autodeterminação e os direitos de personalidade. Estes últimos vinculados à noção de livre desenvolvimento da personalidade, privacidade e autodeterminação informativa.

Para a compreensão dessa relação, urge mencionar que o direito à autodeterminação informativa consiste em um direito do indivíduo de decisão[51], quanto aos seus próprios dados e informações. Ou seja, esta prerrogativa certifica que o titular tenha domínio sobre os seus dados pessoais, mesmo que isso não ocorra de modo absoluto.

Assim, analisando a questão sobre as lentes do conceito de dignidade, a proteção destes dados pessoais envolve, também, a salvaguarda da possibilidade concreta do desenvolvimento pessoal e da autonomia quanto a gestão dos seus dados, materializando a garantia de uma esfera privada e íntima, a qual é indispensável.

Ademais, Sarlet aponta que este direito possui duas dimensões, uma individual e a outra coletiva. A primeira possibilita que cada um decida sobre o acesso, uso e difusão de seus dados, enquanto a segunda versa sobre a autodeterminação informativa enquanto condição prévia para “uma ordem comunicacional livre e democrática”, distanciando-se, de uma concepção de privacidade individualista e mesmo isolacionista.

Portanto, uma adequada salvaguarda dessa protetiva é requerida para a efetiva estruturação de um Estado Democrático de direito. Ora, por meio da transformação social ocasionada pela adoção de uma economia social, bem como pelo advento das tecnologias tem-se a diluição dos contornos entre público e privado. Essa quebra de liames bem definidos apresenta riscos consideráveis à uma estrutura democrática, caso não sejam preservados alguns cernes da esfera privada do indivíduo.

Posto que, inexistindo esse espaço privado não haveria abertura para a estruturação de uma individualidade sem a interferência externa. Sendo destruída a ideia de um “Eu” per si, dando espaço exclusivamente a um “Eu” social. Culminando, pois, na eliminação da diversidade humana, posto que cada pessoa agiria em ampla conformidade com a dinâmica coletiva, não sobrando espaço para qualquer exclusividade.

Promovendo uma verdadeira padronização, a qual é completamente incompatível com um sistema democrático que prioriza a gestão de uma pluralidade de ideias e projeções. Daí a necessidade da proteção da esfera privada. Esta que representa o âmago do indivíduo, estabelecendo um espaço onde não há interesse de terceiros.

---

[51] *Ibid.,* p. 49.

Diante do exposto, tomando por base a supramencionada relevância da salvaguarda da esfera privada do indivíduo, passa-se a analisar a interferência destes dados para a formação da personalidade do indivíduo. Delineando, depois, alguns contornos específicos quanto às questões inerentes à privacidade e à intimidade.

2.1.3 Da personalidade

Partindo dos pressupostos outrora discutidos, cabe direcionar a análise subsequente para uma compreensão mais ampla quanto a interferência dos dados, em especial os sensíveis, na projeção da personalidade do indivíduo. Para tanto, mostra-se como relevante tecer algumas considerações quanto a aspectos basilares que permeiam a noção de personalidade.

Inicialmente, deve-se observar a função dos mencionados direitos da personalidade. Para Bioni[52], esta se traduz em promover e assegurar o valor-fonte[53] do ordenamento jurídico, qual seja, a pessoa humana que se encontra respaldada por um sistema ou uma cláusula geral de proteção. Para o autor a personalidade perpassa pela ideia de características ou o conjunto de características que distingue uma pessoa da outra. Partindo desse pressuposto, os direitos da personalidade seriam os caracteres incorpóreos e corpóreos que conformam a projeção da pessoa humana[54].

Ademais, para o doutrinador Silvio Romero Beltrão[55], os direitos da personalidade fazem referência a um conjunto de bens que são tão próprios do indivíduo, que chegam a se confundir com ele mesmo. Assim, o autor define tais direitos como uma categoria especial de direitos subjetivos que, “fundados na dignidade da pessoa humana garantem o gozo e o respeito ao seu próprio ser, em todas as suas manifestações espirituais ou físicas”.

---

[52] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019.

[53] Miguel Reale dirá que a pessoa-humana é um valor-fonte. Pondera que os valores não possuem uma existência em si ontológica, mas seriam provenientes da experiência humana, especialmente por meio da história a se tornar uma invariante axiológica. Por esse raciocínio, é que Bioni chega ao princípio da dignidade da pessoa humana e aos direitos da personalidade em virtude da travessia por ele projetada, especialmente por conta dos episódios históricos terrificantes que conformam esse horizonte de proteção do ser humano.

[54] REALE, Miguel. **Filosofia do direito**. São Paulo: Saraiva, 2002. p. 208-214.

[55] BELTRÃO, Silvio Romero. Direito da Personalidade: Natureza Jurídica, Delimitação do Objeto, Relações com o Direito Constitucional. *In:* MENEZES, J. B. (Org.). **Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira**. 1 ed. Florianópolis: Conceito, 2010, v. 1, p. 471-489.

Para Ascensão[56], pode-se dizer que a pessoa é o bem supremo da ordem jurídica, o seu fundamento e seu fim. Especialmente considerando o outrora mencionado princípio da dignidade da pessoa humana. Concluindo, pois, que o Estado existe em função das pessoas e não o contrário, ou seja, a pessoa é o sujeito do direito e nunca o seu objeto.

A orientação finca-se no pressuposto da adoção de um direito privado despatrimonializado ou repersonalizado, o qual deve constantemente buscar a tutela do indivíduo em uma sociedade naturalmente multável. Nesse interim, com o advento das novas tecnologias, fica evidente que a protetiva supra vem passando por diversos desafios inéditos.

Desse modo, em virtude da reiterada relevância dos mencionados preceitos, principalmente no que concerne à esfera de autodeterminação individual, Bioni[57] entende que a ciência jurídica deve os proteger das agressões as quais estão sujeitos. De modo a conferir tutela jurídica aos elementos que emprestam conteúdo ao valor-fonte do ordenamento jurídico.

Nesse diapasão, as informações e os dados que estejam atrelados à esfera em questão podem ser inseridos dentre os direitos da personalidade[58], uma vez que se caracterizam como uma projeção, extensão ou dimensão do seu titular, estabelecendo, portanto, uma nova modalidade de identidade. Esta que, por sua vez, assegura, por exemplo, que uma pessoa exija a retificação de seus dados pessoais para que a sua projeção seja precisa, conforme dispõe os arts. 6º, V, e 8º, III, ambos da LGPD, dentre outras protetivas.

Ademais, o autor[59] explica que, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas, posto que vivemos em uma sociedade que se orienta e movimenta a partir desses signos identificadores do cidadão. Assim, os dados pessoais não estão relacionados somente com a privacidade, haja vista que repercutem em mais de uma das espécies dos direitos da personalidade.

Cabendo ressaltar que a proteção dos dados em comento transcende a percepção trazida pelo direito à privacidade. Ora, conforme outrora analisado, este eixo está ligado ao controle de informações pessoais, respaldando as estruturas íntimas ou privadas do sujeito.

---

[56] ASCENSÃO, José de Oliveira. **Teoria Geral do Direito Civil**. Coimbra: Editora Coimbra, 1997.
[57] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 51.
[58] *Ibid.,* p. 52.
[59] *Ibid.,* p. 55.

Já aquela protetiva não se satisfaz com tal técnica normativa, posto que existe, por exemplo, a possibilidade de a questão referente aos dados visar apenas discutir a correção de informações que estejam sob a esfera pública, o que perpassa pela dinâmica da identidade e não da privacidade.

Rabindranath[60], em sua obra o Direito Geral de Personalidade, dispõe que o bem da identidade reside na própria ligação de correspondência do homem consigo mesmo e, portanto, atrela-se às profundas necessidades humanas, de modo que o teor da convivência humana acaba dependendo de sua salvaguarda em termos de reciprocidade. Nesse sentido, Bioni completa delimitando que as informações que influem na projeção de uma pessoa e na sua esfera relacional adéquam-se conceitualmente como um novo direito da personalidade. Desse modo, vislumbra-se a necessidade de tutelada destes.

O Código Civil de 2002 estabelece um relevante norte para a protetiva supramencionada, dimensionado a existência de um caráter tanto intransmissível, não podendo ser objeto de cessão ou sucessão, como também irrenunciável desse direito, não sendo possível abdicar dele, mas apenas restringir.

Beltrão[61] acrescenta que os direitos da personalidade são pessoais em face de seu caráter não patrimonial, porém os bens por ele tutelados possuem uma correlação imediata com o interesse econômico. Isto, porque há um reflexo patrimonial nos direitos em questão, especialmente quando se observa os remédios contra lesões à personalidade. São aplicadas medidas que visem a cessação da ofensa e a reintegração especifica do bem violado, acrescido do ressarcimento patrimonial.

Nesse sentido, Menezes de Cordeiro[62] destaca três relevantes distinções para a matéria. Sendo a primeira categoria representada por um sentido forte do aspecto não patrimonial, segundo a qual os direitos da personalidade não admitiriam que os bens tutelados sejam permutados por dinheiro, a exemplo da vida e da saúde.

Outrossim, categoriza um sentido mais fraco, porém ainda não patrimonial da protetiva em comento, em que se admite o surgimento de determinados negócios

---

[60] CAPELO DE SOUSA, Rabindranath Valentino Aleixo. **O direito geral de personalidade**. Coimbra: Coimbra Editora, 2011, p. 245.
[61] BELTRÃO, Silvio Romero. Direito da Personalidade: Natureza Jurídica, Delimitação do Objeto, Relações com o Direito Constitucional. *In:* MENEZES, J. B. (Org.). **Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira**. 1 ed. Florianópolis: Conceito, 2010, v. 1, p. 471-489.
[62] CORDEIRO, Antônio Menezes. **Tratado de Direito Civil Português**. Coimbra: Almedina, 2007.

patrimoniais ou com algum alcance com esse viés, isso dentro de determinadas regras preestabelecidas. A exemplo dos esparsos casos de experimentação humana.

A última distinção trazida por Cordeiro é a vertente patrimonial, na qual o direito pode ter representação pecuniária e ser negociado, como no caso da utilização consentida do nome, imagem e o fruto da atividade intelectual.

Contudo, a sociedade cada vez mais conectada vem encontrando mecanismos cada vez mais sofisticados de mobilização de dados para fins econômicos. Assim, o que pode parecer inofensivo sob uma perspectiva inicial, acaba se convertendo em uma ameaça considerável.

Exemplos evidenciam-se com o uso indevido a dados sensíveis dos indivíduos, culminado em graves situações como empresas de planos de saúde ou seguradoras potencialmente modificando negativamente a cobertura que ofertada em detrimento de informações privilegiadas quanto ao quadro de saúde da pessoa, ou mesmo a estruturação de golpes e fraudes utilizando tais dados indevidamente obtidos.

Para além dessas questões, urge analisar alguns aspectos específicos quanto à privacidade, a distinguindo dos contornos das esferas intimas, para que haja uma adequada compreensão quanto a influência dos dados pessoais sob essas estruturas.

2.1.4 O direito à intimidade e à privacidade

No ordenamento jurídico brasileiro[63], existiram previsões a respeito da proteção aos direitos fundamentais em Constituições anteriores, as quais recaem indiretamente na privacidade, como a inviolabilidade do domicílio e o sigilo das correspondências. Entretanto, apenas com a Constituição Federal de 1988 houve uma referência expressa à vida privada e à intimidade. Essa proteção constitucional foi concedida não somente para tutelar a relação entre o indivíduo e o Estado, mas, também, entre os particulares.

Nesse interim, analisando a normativa constitucional, percebe-se a presença de direitos fundamentais que buscam atingir a promoção e defesa da personalidade. Entre

[63] OLIVEIRA, Rodrigo da Costa de. Direito a intimidade e sua proteção baseada nos direitos humanos no mundo. **Âmbito Jurídico**. 2014. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/direito-a-intimidade-e-sua-protecao-baseada-nos-direitos-humanos-no-mundo/#_ftn7. Acesso em: 28 dez. 2023.

eles, é possível citar: o princípio da dignidade da pessoa humana[64]; os direitos à vida, à liberdade e à igualdade[65]; e os mencionados direitos à intimidade, à vida privada, à honra e à imagem[66].

Já o Código Civil traz, em seu rol das inovações, um capítulo chamado “Dos Direitos da Personalidade”. Este possui onze artigos, com uma posição topográfica relevante, tendo em vista que se delineia dos artigos 11 ao 21, o que demonstra, de certa forma, um ordenamento que possui como valor máximo a proteção da pessoa humana.

O Brasil declarou expressamente no artigo 5º, inciso X, da CF a proteção ao direito à privacidade quando determinou que: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”[67].

Assim, não é forçoso perceber que se tratam de direitos de fundamental tutela. Cabendo, pois, uma análise mais minuciosa sobre suas disposições, inclusive para a compreensão das escolhas legislativas expostas.

Partindo dos pressupostos trazidos e sem a intenção de estabelecer um conceito fechado sobre o tema, Celso Ribeiro Bastos[68] traz uma noção de privacidade como a faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhe o acesso a informações privadas de cada um, evitando que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

Para Rogério Donizetti[69], a privacidade consiste no grupo de modo de viver e de ser, em que se estabelece o direito que a pessoa tem de viver a sua própria vida. Equivale, ainda, a possibilidade que cada indivíduo possui de impedir a interferência dos estranhos na sua vida familiar e privada, bem como de obstar o acesso a informações sobre a vida

---

[64] BRASIL. **Constituição (1988).** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 maio 2024.
[65] *Ibid.*
[66] *Ibid.*
[67] *Ibid.*
[68] BASTOS, Celso Ribeiro Bastos. Tribunal Regional Federal da 1ª Região. **A Constituição na Visão dos Tribunais - Interpretação e Julgados - Artigo por Artigo**. v. 1. Brasília: Editora Saraiva, 1997, p. 30.
[69] OLIVEIRA, Rodrigo da Costa de. Direito a intimidade e sua proteção baseada nos direitos humanos no mundo. **Âmbito Jurídico**. 2014. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/direito-a-intimidade-e-sua-protecao-baseada-nos-direitos-humanos-no-mundo/#_ftn7. Acesso em: 28 dez. 2023.

privada de cada um e a divulgação de informações sobre esta zona de manifestação existencial.

Essas noções assumem uma perspectiva de liberdade negativa, na qual o indivíduo não sofre interferência alheia. Entretanto, essa noção ganhou novos e mais amplos contornos. A exemplo do que defende Caitlin Mulholland. Para a autora existem três concepções sobre o direito à privacidade, as quais englobam: o direito de ser deixado só, o direito de ter controle sobre a circulação dos dados pessoais, e o direito à liberdade das escolhas pessoais de caráter existencial.

Nesse sentido, acrescenta Rodotà[70] que a privacidade deve ser considerada como o direito de manter o controle sobre suas próprias informações e de "determinar a maneira de construir sua própria esfera particular". Possibilitando a chamada autodeterminação informativa e a realização plena de sua liberdade existencial.

Examinando o direito à privacidade, tem-se que ele antecede o *Bill of Rights*, já que pode ser encontrado em certos códigos mais antigos, em escritos filosóficos e, também, nas tradições. Além disso, é possível encontrar alguns traços na Bíblia, quando se trata da vergonha que Adão e Eva sentiram pela violação da privacidade, tal como no caso de Noé, em relação à nudez do seu pai. Mesmo com as conhecidas distinções que existem entre os conhecimentos científicos e os conhecimentos mitológicos e religiosos.

Beltrão aponta que esses apontamentos são relevantes para demonstrar como a proteção da intimidade está relacionada à ideia de individualidade, além de evidenciar como são transcendentais e interdisciplinares os valores protegidos pelo direito à privacidade[71].

O caso precursor principal a tratar sobre o tema na Suprema Corte Americana foi o de Griswold *versus* Connecticut, que foi responsável por julgar uma proibição presente na Lei de Comstock, marcada por determinar que as pessoas não fizessem uso de artigo medicinal ou medicamento para prevenir a concepção, tendo como base a Constituição do país. Essa Lei foi considerada inválida pela Suprema Corte por ir de encontro à privacidade conjugal, tutelando, dessa forma, as práticas íntimas[72].

---

[70] RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.
[71] BELTRÃO, Silvio Romero. Direito da Personalidade: Natureza Jurídica, Delimitação do Objeto, Relações com o Direito Constitucional. *In:* MENEZES, Joyceane Bezerra. (Org.). **Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira**. 1 ed. Florianópolis: Conceito, 2010, v. 1, p. 471-489.

[72] *Ibid.,* p. 1395.

Assim, o direito à privacidade tem sido estruturado sobre o arcabouço da dicotomia entre as esferas pública e privada. Cujos contornos desta seriam, para Bioni[73], estabelecidos na habitação privada, enquanto o espaço para que as pessoas se refugiassem do escrutínio público. O autor entende que a esfera privada em questão seria um espaço de reflexão, um refúgio que evitaria um nivelamento social dos indivíduos e, em última análise, a "instalação de visões totalitárias".

Somente com o que o autor chamou de fuga da "pressão social", os indivíduos conseguiriam desenvolver a sua subjetividade, a qual seria projetada em meio à sociedade. Ressaltando, pois, que se trata de um conceito basilar à própria democracia e condição essencial ao livre desenvolvimento da personalidade dos cidadãos.

Partindo dessas disposições e imbuídos da relevância da protetiva outrora mencionada, para fins didático, cabe destacar as distinções entre dois conceitos autônomos, mas correlacionados, quais sejam: a intimidade e a privacidade.

René Ariel Dotti[74] destaca que a intimidade está inserta na vida privada como se elas fossem dois círculos, assim dizendo, uma teoria dos círculos concêntricos. Segundo a qual, a intimidade consiste em um círculo concêntrico de menor raio em comparação com a vida privada. Dessa maneira, quanto mais próximas das informações a revelar estiverem as esferas de intimidade e segredo, maior será o peso que terão que incumbir as razões para alcançar a sua revelação, da perspectiva do interesse público.

Entre tantos exemplos, é importante destacar que Paulo Lôbo[75] afirma que o direito à privacidade é gênero, em que se inserem as espécies: direito à intimidade, direito à vida privada, direito ao sigilo e direito à imagem. Contrário a isso, Carlos Alberto Bittar[76] acredita que o direito à intimidade é gênero, que compreende a proteção, entre outros, à privacidade, ao segredo e à imagem. Bruno Lewicki[77], a respeito dessas discordâncias, sintetiza dizendo que tais direitos consistem em um aglomerado que compreende interesses díspares relacionados à proteção da vida privada.

---

[73] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 06 jan. 2024.
[74] DOTTI, René Ariel. **Curso de direito penal**. Rio de Janeiro: Forense, 2001.
[75] LÔBO, Paulo. **Direito Civil: parte geral**. São Paulo: Saraiva, 2015, p. 139.
[76] BITTAR, Carlos Alberto. **Os direitos da personalidade**. 2. ed. Rio de Janeiro: Forense Universitária, 1995, p. 102.
[77] LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003, p. 31.

Assim, ultrapassada essa distinção e partindo da perspectiva que o direito à privacidade possui um raio maior de atuação, bem como a evidente relevância da sua adequada tutela, passa-se a considera-la como pressuposto para a vertente pesquisa quanto a acesso indevido a dados sensíveis dos pacientes e suas consequências.

Ora, levando em consideração que o direito à privacidade é uma espécie do direito da personalidade e que é preciso somente ser pessoa para ser titular desse direito, percebe-se que a privacidade também deve ser prestigiada em âmbito clínico e hospitalar[78]. Cujo enfoque é ainda mais significativo pela natureza dos dados ali veiculados.

Cabe, antes de analisar algumas minúcias desse setor, tratar do que Anderson Schreiber[79] chamou de interferência da evolução tecnológica no setor da Privacidade. Para o autor, a propagação de meios para recolher, armazenar, processar e utilizar a informação incentivam a massificação dos contratos e o crescimento exponencial da quantidade dos dados na sociedade contemporânea.

Aliado a isso, Maria Celina Bodin Moraes e Carlos Nelson Konder[80] afirmam que, entre as questões da personalidade, seguramente a privacidade é a que sofreu as transformações mais profundas em decorrência do avanço das tecnologias invasivas e, também, da indiscrição e da curiosidade da sociedade civil em relação à vida privada das pessoas.

Celso Ribeiro Bastos[81] alerta que:

> […] a evolução tecnológica torna possível uma devassa na vida íntima das pessoas. (…) Nada obstante, na época atual, as teleobjetivas, assim como os aparelhos eletrônicos de ausculta, tornam muito facilmente devassável a vida íntima das pessoas. (…) Sem embargo, disso, sentiu-se a necessidade de proteger especificamente a imagem das pessoas, a sua vida privada, a sua intimidade.

Frente a essa realidade, é possível separar a problemática referente à privacidade em duas dimensões. A primeira é procedimental, que abrange o alcance e o tratamento do dado pessoal. Ao passo que a segunda é substancial, de modo que compreende e trata a

---

[78] BELTRÃO, Silvio Romero. Direito da Personalidade: Natureza Jurídica, Delimitação do Objeto, Relações com o Direito Constitucional. *In:* MENEZES, Joyceane Bezerra. (Org.). **Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira**. 1 ed. Florianópolis: Conceito, 2010, v. 1, p. 471-489.
[79] SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2013. p. 135.
[80] KONDER, Carlos Nelson; MORAES, Maria Celina Bodin de. **Dilemas de direito civil-constitucional: casos e decisões**. Rio de Janeiro: Renovar, 2012, p. 267.
[81] BASTOS, Celso Ribeiro Bastos. **Curso de direito constitucional**. São Paulo: Saraiva, 1997, p. 194.

utilização que se faz do dado pessoal, resultando, em algumas hipóteses, em transgressões a outros direitos da personalidade[82].

Portanto, fica evidente a relevância da observância adequada ao preceito que dispõe sobre a privacidade do indivíduo. Inclusive, enquanto manifestação intimamente vinculada com a própria protetiva constitucional da proteção a dignidade da pessoa humana e a efetiva construção da identidade em um cenário proporcionado pelo estado democrático de direito.

Um outro aspecto relevante para um adequado aprofundamento sobre o tema perpassa pela análise do sigilo médico, enquanto pressuposto da lealdade profissional e, por consequência, da adequada prestação do serviço médico-hospitalar. Passa-se, pois, a análise deste.

2.1.5 A relevância do sigilo médico enquanto pilar da relação médico-paciente

Nesse diapasão, urge-se delinear sobre algumas das protetivas supramencionadas com o fito de dimensionar a relevância da garantia de sua tutela. Inicialmente, tem-se o caro sigilo médico, o qual pode ser compreendido como um dos pilares da tradição médica.

A notória preocupação com a normatização desse preceito finca-se no pressuposto básico de que garantindo a proteção das informações pessoais atinentes ao paciente haveria, por conseguinte, a salvaguarda da lealdade profissional, enquanto fator que reforça a credibilidade de certas profissões, promovendo a confiança necessária para o bom funcionamento destas atividades.

Normalmente, o convívio em sociedade gera a necessidade de valer-se do auxílio de terceiros, que são pessoas determinadas para as quais é inescusável expor fatos íntimos, que almejava manter em segredo. Em vista disso, José Henrique Pierangeli afirma que:

> A vida mantida em meio a uma comunidade apresenta fatos e problemas para cuja solução temos de recorrer a terceiros, pessoas qualificadas técnica e profissionalmente para removê-los, e as pessoas que exercem certos ministérios, aos quais se confiam segredos da intimidade pessoal ou doméstica, que devem ser

[82] SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2013, p. 138.

> mantidos em sigilo não só em benefício do cidadão confidente, mas da própria convivência social, interesses de ordem natural, moral, social ou econômica.[83]

Nesse sentido, determinados segmentos profissionais são consagrados como confidentes necessários, isto é, no suceder do exercício de seus trabalhos, esses profissionais tem contato direto com informações de caráter íntimo e confidencial de terceiros.

A exemplo de advogados, médicos e até mesmo padres que testemunham verdadeiras confissões de pecados, os profissionais, em diferentes níveis, devem proteger as informações reveladas no exercício profissional.[84] À vista disso, faz-se fundamental o sigilo profissional, com o intuito de assegurar o uso desses serviços de modo eficiente e resguardado, com a proteção de poder expor confidências íntimas, sem o perigo de vê-las reveladas, gerando, por consequência, futuros constrangimentos.[85]

No que diz respeito especificamente ao sigilo no âmbito médico, Louise Santiago[86] destaca que consiste em uma espécie de segredo profissional, consagrado no Direito, que atua como um dos princípios mais honrados e prezados pelos médicos. Hercules Sidnei Pires Liberal traz o seguinte conceito de segredo médico:

> É o segredo médico uma espécie de segredo profissional, devido pelos denominados confidentes necessários, cujas confidências são expostas por imperiosa necessidade de busca de auxílio para reparação de um estado mórbido ou de lesões de ordem moral ou patrimonial. Alinham-se, neste caso, os sigilos impostos aos profissionais que, para prestação de qualquer tipo de serviço, necessitem penetrar na intimidade do cliente.[87]

O preceito é respaldado por um dos mais antigos documentos que orienta a atuação profissional do exercício da medicina: O Juramento de Hipócrates, onde lê-se: “O que, no exercício ou fora do exercício e no comércio da vida, eu vir ou ouvir, que não seja necessário revelar, conservarei como segredo” (460 a.C.).

---

[83] PIERANGELI, José Henrique. **Manual de direito penal brasileiro, v. 2: parte especial: arts. 121 a 361**. 2. ed. rev., atual., ampl. e compl. São Paulo: Editora Revista dos Tribunais, 2007, p. 187-188.
[84] DE PAULA, Alexandre Sturion. Digressões sobre a violação do sigilo profissional. **Portal Universo Jurídico**, 2002. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/10736-10736-1-PB.htm. Acesso em: 30 nov. 2023.
[85] SANTIAGO, Luiz Carlos Figueiredo. O sigilo médico e o direito penal. **Revistas UNIFACS**, Salvador, n. 128, fev. 2011. Disponível em: https://revistas.unifacs.br/index.php/redu/article/viewFile/1409/1096. Acesso em: 29 nov. 2023.
[86] *Ibid.,* p. 08.
[87] LIBERAL, Horácio Silva Pires. Sigilo Profissional. **Portal CFM**, 1993. Disponível em: http://www.portalmedico.org.br/include/biblioteca_virtual/des_etic/10.htm. Acesso em: 29 dez. 2023. p. 01.

Complementando o conceito hipocrático, os autores Marcos de Almeida e Daniel Munhoz[88] elencam três razões principais que justificam o dever de sigilo profissional por parte do médico. A primeira delas, consiste em uma razão utilitária, fundamentada no juízo de que a confidencialidade médica encoraja o enfermo a buscar atendimento médico sem receio de estigmas ou eventuais reverberações sociais negativas que possam ocorrer com o conhecimento público do seu caso clínico, conforme outrora mencionado. Ademais, tal incentivo colabora para o diagnóstico precoce de doenças e contribui para a construção de uma sociedade mais saudável.

Os autores ainda defendem que tal contexto contribui para o desenvolvimento da confiança mútua entre médico e paciente, o que é substancial para um bom rendimento do tratamento clínico, além de que a privacidade e a confiança criam atmosfera necessária para o desenvolvimento não apenas da relação médico-paciente, mas como de todas as relações humanas[89]. Além disso, destaca-se que a ausência ou a quebra de confiança dentro da relação médica, além de frustrar o vínculo entre as partes, pode acarretar prejuízos nos cuidados com a saúde do paciente, bem como possui o condão de gerar "danos morais e patrimoniais irreparáveis aos doentes, cidadãos e ao próprio exercício da medicina".[90]

Outrossim, é possível enumerar a segunda razão para o sigilo profissional com relação direta a um caráter jurídico-contratual da relação médico-paciente. Isto é, sempre que um indivíduo procura um estabelecimento de saúde para atendimento médico, pressupõe-se a existência de um contrato expresso ou implícito que guia esta relação. Sob o manto desse contrato, o médico se dispõe a manter as informações prestadas em segredo e fazer uso profissional desses dados, isso porque além do contrato com o paciente, existe um aparato normativo que protege a intimidade e privacidade do paciente.

Desse modo, a Constituição Federal proporciona "a expansão e consolidação de uma nova consciência jurídica dos cidadãos, calcada primordialmente na efetividade dos

---

[88] ALMEIDA, Maria; MUNHOZ, Damião Rodrigues. O princípio e as razões do segredo médico. **Revista IMESC**, São Paulo, n.1, dez. 1998.

[89] LOCH, Jacqueline Azevedo. Confidencialidade: natureza, características e limitações no contexto da relação clínica. **Revista Bioética**. Brasília. v. 11. p. 514. nov. 2003. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/149/153. Acesso em: 11 dez. 2023.

[90] GONÇALVES, José Luiz Ramalho. Algumas considerações sobre segredo médico e segredo profissional de advogado (em Portugal e no Brasil). **Revista CEJ**, v. 3 n. 7 jan./abr. 1999, p. 100-107. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/184/346. Acesso em: 11 dez. 2023.

direitos” [91]. Assim, firmando *status* de direito fundamental à inviolabilidade da intimidade, da vida privada, da honra e da imagem dos indivíduos. Nesse diapasão, o doutrinador José Afonso Silva, em sua obra Curso de Direito Constitucional Positivo[92], destaca que a inviolabilidade descrita abarca todas as manifestações da esfera íntima, da vida privada e da personalidade, denominando-as de direito à privacidade.

Assim, a salvaguarda das prerrogativas constitucionais que tutelam não somente os mencionados dados individuais, mas também, de modo mais abrangente, o direito à intimidade do indivíduo é essencial para que tal paciente se sinta confortável o suficiente para compartilhar com o profissional da saúde as informações fundamentais para o tratamento daquele. Desse modo, é notória a relevância de tal preceito para a razoável manutenção da mencionada atividade.

Dessarte, o preceito constitucional de proteção à privacidade se irradia em todo o ordenamento jurídico, com expressão em diversos dispositivos legais. O art. 154 do Código Penal (CP), por exemplo, define o crime de violação de segredo profissional, punindo com detenção, de três meses a um ano ou multa, aqueles que revelarem, sem justa causa, segredo que tenha tido conhecimento em razão da função, ministério, ofício ou profissão[93].

No mesmo sentido, os arts. 388 e 448 do Código de Processo Civil[94] e art. 247 do Código de Processo Penal (CPP) dispõem sobre a proibição da prestação de testemunho de pessoas que, em razão de sua função, ministério, ofício ou profissão, devam guardar segredo.

O Código de Ética Médica brasileiro[95], por sua vez, se dedica do art. 73 ao 79 a dispor sobre a atuação médica em relação ao sigilo profissional, vedando-lhes expor fatos sobre o paciente que se teve conhecimento no exercício da profissão. A notória preocupação com a normatização desse preceito finca-se no pressuposto básico de que garantindo a proteção das informações pessoais atinentes ao paciente haveria, por

---

[91] GRECO, Leonardo. O processo de execução. Rio de Janeiro: Renovar, 1999. p. 1

[92] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 41. ed., ver. e atual. São Paulo: Malheiros, 2018.

[93] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 maio 2024.

[94] BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Diário Oficial da União, Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 29 maio 2024.

[95] CONSELHO FEDERAL DE MEDICINA (CFM). **Código de Ética Médica**. Brasília, DF: CFM, 2018. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 29 maio 2024.

conseguinte, a salvaguarda da lealdade profissional, enquanto fator que reforça a credibilidade de certas profissões, promovendo a confiança necessária para o bom funcionamento destas atividades.

Parte-se para a análise da terceira razão que fundamenta o sigilo, qual seja, a razão da privacidade. Almeida e Munhoz[96] defendem que a privacidade deve implicar ao indivíduo o poder de controle acerca das informações e dados sobre si mesmo, como uma expressão da autonomia e exercício de autodeterminação[97]. Assim, a violação de sigilo afronta o poder pessoal de eleger quais informações e aspectos da vida privada se deseja levar a público, ameaçando todas as esferas das relações humanas.

Quando se trata da relação médica, o profissional possui, em determinado grau, um poder sobre o paciente, já que detém ciência sobre informações relacionadas direta ou indiretamente a aspectos da vida, como particularidades sobre hábitos de vida e bases relacionadas a doença, sintomas ou lesão que originou a busca pelo tratamento médico. As informações prestadas no atendimento médico se mostram do tipo mais íntimo possível, visto que os dados obtidos em um exame físico ou de anamnese representam uma extensão do corpo ou da mente do indivíduo.[98]

Nessa perspectiva, Paulo Vinícius Sporleder de Souza destaca:

> O segredo médico é um procedimento típico e inerente às profissões ligadas às ciências médicas. A natureza confidencial do relacionamento médico-paciente é aceita como da maior relevância e exigida pela sociedade como forma de proteção. É interesse social que os fatos da vida privada revelados pelos pacientes sejam resguardados, ocultados, isto é, sejam mantidos em segredo pelo médico, pois, do contrário, sem esse sigilo, poucas pessoas se arriscariam a procurar ajuda desses profissionais.[99]

Isto posto, verifica-se, portanto, que as concepções basilares do sigilo profissional estão em consonância com ideais de utilidade, com viés a objetivar a eficiência do tratamento e o firmamento da confiança mútua entre as partes. Bem como um imperativo

---

[96] ALMEIDA, Maria; MUNHOZ, Damião Rodrigues. O princípio e as razões do segredo médico. **Revista IMESC**, São Paulo, n.1, dez. 1998.

[97] LOCH, Jacqueline Azevedo. Confidencialidade: natureza, características e limitações no contexto da relação clínica. **Revista Bioética**. Brasília. v. 11. p. 51-64. nov. 2003. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/149/153. Acesso em: 11 dez. 2023.

[98] *Ibid.,* p. 64.

[99] SOUZA, Paulo Vinícius Silva de. **Direito Penal Médico**. Porto Alegre: Livraria do Advogado Editora, 2009, p. 90.

de ordenação jurídica, com desígnio de efetivar a proteção à privacidade, repousando assim, sob justificativa que concilia a natureza ética e legal.

Todavia, apesar do denso arcabouço teórico acerca do dever do sigilo médico, este não é capaz de formular regras absolutas, havendo casos em que a intervenção no sigilo médico e o compartilhamento de certos dados se mostra essencial a defesa de direitos do titular desses dados. Desse modo, é possível notar a instituição de limites para o sigilo médico.

Os dispositivos normativos já apresentados anteriormente, ao disporem sobre o segredo profissional, evidenciam a existência dessas limitações à protetiva da confidencialidade e privacidade. Ora, tais regramentos, a exemplo do Código de Ética Médica, impõem a vedação ao ato de revelar a alguém segredo de que se tenha tido ciência, em razão do exercício profissional, no entanto prevê exceções a essa regra desde que fundamentadas por motivo de justa causa, dever legal ou consentimento, por escrito, do paciente, ou ainda quando a não revelação possa acarretar dano ao paciente.[100]

Desse modo, a obra Direito Médico[101], de Genival Veloso França, traz que a concepção de “justa causa” está inserida dentro da noção do bem social, quando capaz de legitimar um ato proibido. Haja vista que está voltada aos interesses coletivos e defendida por preocupações condizentes com as prerrogativas conquistadas pela sociedade organizada. Estando não apenas prevista em lei, como também explícita no estado de necessidade, na legítima defesa, no exercício regular do direito e no estrito cumprimento do dever legal.

Em efeitos práticos, o compartilhamento de dados do paciente que estejam sob a proteção do sigilo profissional pode ser flexibilizado em casos que a legislação estabelece a notificação compulsória de determinadas doenças transmissíveis. Além disso, sob a guarda do princípio da não-maleficência, tem-se, por exemplo, os casos em que houver suspeita de violência doméstica e familiar contra idosos ou cônjuges, ou suspeita de abuso ou agressão contra crianças e adolescentes, em que haja probabilidade de dano físico ao paciente.

---

[100] CONSELHO FEDERAL DE MEDICINA (CFM). **Código de Ética Médica**. Brasília, DF: CFM, 2018. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 29 maio 2024.

[101] FRANÇA, Genival Veloso de. **Direito médico**. 12. ed., rev., atual., e ampl. Rio de Janeiro: Forense, 2014.

Ressalta-se, no entanto, que ante o conflito entre os princípios da privacidade e o dever do sigilo profissional, não há um princípio universal que prevaleça, devendo-se analisar as particularidades de cada caso concreto com viés de razoabilidade, com foco na proteção da integridade do indivíduo. Ainda, sempre que existir pressupostos que tornem inevitável a quebra do sigilo médico, o profissional deve deixar claro e fazer constar que a revelação das condições ou do diagnóstico do paciente foi a pedido do próprio ou de seus responsáveis legais, ou descrever a hipótese de interesse público que o motivou. Assim, a violação do segredo deve ser avaliada de acordo com os interesses de todos os envolvidos no caso prático.[102]

A valer, o dever do sigilo não pode se sobrepor aos interesses públicos protegidos pela Justiça e ordenamento jurídico, que tem escopo de garantir o bem-estar social. Em vista disso, França[103] destaca, então, que a "justa causa" constitui um interesse de ordem social ou política que fundamenta o descumprimento do sigilo, mesmo que essa violação implique em um certo cerceamento de um avanço da liberdade individual, tendo em vista que privacidade individual consiste em um princípio prestigiado nas sociedades organizadas, além de ser imperativo constitucional. Dessa forma, percebe-se que o conceito de segredo médico é relativo, uma vez que se defende a tutela do bem comum e o equilíbrio social, e não a vontade individualista de cada um pontualmente. Importante ressaltar que a proibição da lei é a da revelação ilegal, que tenha como fundamento a má-fé e a leviandade. Então, o fundamento do sigilo médico é impedir a exposição desnecessária de informações e dados que tenham condão de acarretar prejuízos morais e financeiros para o paciente, ou que, simplesmente não seja da vontade do indivíduo de expô-los, como exercício de sua autonomia.

Sendo assim, o entendimento que tem prevalecido é o de que o sigilo médico é relativo, devendo as revelações estarem embasadas em razões legais, éticas e sociais, além de que isso deve acontecer com uma certa moderação e em situações específicas do exercício da medicina, quando se afirma que essa violação foi exigida por conta de um interesse maior.

Não se pode esquecer de mencionar que os avanços tecnológicos e o desenvolvimento de ferramentas facilitadoras de manuseio e compartilhamento de dados,

---

[102] FRANÇA, Genival Veloso de. **Direito médico**. 12. ed., rev., atual., e ampl. Rio de Janeiro: Forense, 2014.
[103] *Ibid.,* p. 45.

bem como a implementação de sistemas de informação de saúde nas instituições hospitalares representaram novos desafios para a proteção da privacidade dos usuários. O uso de aplicativos de mensagens instantâneas no atendimento médico, como o *Whatsapp* por exemplo, pode colaborar com o envio de dados sensíveis para terceiros, além dos frequentes golpes e fraudes envolvendo o aplicativo que põem em risco os dados dos pacientes sob a guarda desses estabelecimentos clínicos. Isso revela os novos perigos de acesso indevido com ataques e vazamentos de dados pessoais para utilização com fins diversos dos que basearam a sua coleta.

2.1.6 O hospital e o sigilo médico

É cediço que o sigilo médico vincula não apenas a figura do profissional de medicina, mas engloba toda a cadeia de profissionais que prestam atendimento e manuseiam dados e informações referentes a saúde do paciente. Isto porque, a legislação de proteção de dados inclui os dados sobre a saúde na concepção de dados sensíveis, estabelecendo tratamento mais rígido na utilização desses dados, além de preconizar a segurança das informações do titular.

Dentro do contexto clínico-hospitalar, o prontuário médico é o acervo documental revestido de informações sobre os acontecimentos relativos à saúde do paciente e toda a assistência prestada no seu tratamento. A Resolução nº 1.638/2002 do Conselho Federal de Medicina (CFM) reforça que o documento possui caráter legal, sigiloso e científico, bem como proporciona a comunicação entre a equipe multiprofissional e garante a continuidade da assistência médica exercida ao indivíduo[104] Márcia Fernandes define que o prontuário, em regra, pode trazer informações sobre o histórico clínico, medidas, condutas, exames, imagens, laudos e toda informação que seja relevante para o melhor acompanhamento do paciente. Além disso, pode conter também informações relativas à situação social do paciente e família. [105]

---

[104] CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 1.638, de 10 de julho de 2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários. nas instituições de saúde Brasília: CFM, 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 01 dez. 2023.

[105] FERNANDES, Mário Sérgio. **Prontuário eletrônico e a lei geral de proteção de dados**. Migalhas, 02 fev. 2020b. Disponível em: https://www.migalhas.com.br/coluna/migalhas-deprotecao-de-dados/340202/prontuario-eletronico-e-a-lei-geral-de-protecao-de-dados. Acesso em: 09 dez. 2023.

Com efeito, Jussara de Azambuja Loch revela o conflito existente na utilização do prontuário médico no modelo de cuidados hospitalares moderno. Considera que, do ponto de vista assistencial, o prontuário médico como meio de comunicação multiprofissional proporciona ao paciente um atendimento mais amplo e lhe oferece todos os cuidados disponíveis naquela instituição para o instantâneo e correto diagnóstico com o seu devido tratamento. Assevera, no entanto, que houve uma considerável perda de confidencialidade de informações no sentido de que mais pessoas começaram a ter acesso aos prontuários. Isto porque toda a equipe partilha de informações que, originalmente, foi prestada a um profissional específico que, após registrar no prontuário, compartilha com todos os profissionais envolvidos na cadeia hospitalar. [106]

Em vista disso, o Conselho Federal de Medicina incumbiu as instituições de saúde a missão de exercer o papel de guardiãs do prontuário e das informações nele contidas, de modo que “o prontuário do paciente, em qualquer meio de armazenamento, é propriedade física da instituição onde o mesmo é assistido – independentemente de ser unidade de saúde ou consultório -, a quem cabe o dever da guarda do documento”[107]. Dessa maneira, o dever de zelar e prezar pelo sigilo das informações que recai sobre a pessoa física dos profissionais, também incide sobre as instituições de saúde, em todo o sistema de funções envolvidos no atendimento ao paciente. Isto é, tanto hospitais como unidades básicas de saúde e unidades de pronto atendimento, por exemplo, também tem o encargo de garantir a integridade e a privacidade dos dados.

Nesse aspecto, é válido memorar o fato ocorrido no final do ano de 2020, quando houve vazamento de dados no âmbito do Hospital Albert Einstein, no qual atingiu mais de 16 milhões de pessoas que apresentaram suspeita ou diagnóstico positivo para covid-19. Apurou-se que a divulgação dos dados se deu por funcionário cientista de dados quando atualizava plataforma de dados do hospital. Na ocasião, foram expostas informações relacionadas ao Cadastro de Pessoa Física, endereço, telefone e informações sobre

---

[106] LOCH, Jacqueline Azevedo. Confidencialidade: natureza, características e limitações no contexto da relação clínica. **Revista Bioética**. Brasília. v. 11. p. 51-64. nov. 2003. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/149/153. Acesso em: 11 dez. 2023.

[107] CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 1.638, de 10 de julho de 2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Brasília: CFM, 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 01 dez. 2023.

doenças pré-existentes dos pacientes.[108] Importante destacar que o vazamento ocorreu em período que o mundo ainda enfrentava o caos instaurado pela Pandemia de Covid-19, época em que as informações referentes a saúde da população poderiam ser utilizadas para fins impróprios, que não estivesse relacionado a elaboração de medidas para o combate da propagação do vírus.

Episódios como este reforçam que, para além dos profissionais que exercem funções diretamente atreladas a saúde, a obrigação do sigilo se estende a todos os colaboradores envolvidos na rede de atendimento e tratamento a saúde, mesmo que em setores indiretamente relacionados. Toda a cadeia hospitalar deve atender as previsões deontológicos de conduta a fim de garantir uma manipulação ética dos dados dos pacientes.[109]

Nesse sentido, Jussara Loch assevera que:

> Garantir a confidencialidade é da competência dos profissionais e das instituições, em respeito ao direito individual à individual à intimidade. A segurança da informação é um constituinte do sistema de cuidados em saúde, sendo deste, primariamente, a responsabilidade de executá-la.[110]

Desse modo, o que há de se referir é que com a sistematização de normas jurídicas que objetivam proteger os direitos fundamentais de liberdade e de privacidade frente aos avanços tecnológicos, as instituições tem enfrentado obstáculos na gestão dessas informações. O setor hospitalar, por estar perenemente manipulando dados sensíveis dos pacientes, se encontra no centro desse paradigma, no que diz respeito as condutas exigidas e adotadas por essas instituições para manusear e proteger os dados de forma ética e legal.

2.2 DO PRONTUÁRIO DIGITAL

---

[108] O GLOBO. **Funcionário do Einstein vaza dados do Ministério da Saúde e expõe 16 milhões de pacientes com Covid-19.** 26 nov. 2020. Disponível em: https://oglobo.globo.com/brasil/funcionario-do-einstein-vaza-dados-do-ministerio-da-saude-expoe-16-milhoes-de-pacientes-com-covid-19-24766745 Acesso em: 01 dez. 2023.

[109] LOCH, Jacqueline Azevedo. Confidencialidade: natureza, características e limitações no contexto da relação clínica. **Revista Bioética**. Brasília. v. 11. p. 51-64. nov. 2003. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/149/153. Acesso em: 12 dez. 2023.

[110] *Ibid.,* p. 64.

Traçado o panorama outrora exposto, cabe realizar um aprofundamento quanto ao mecanismo hodiernamente utilizado para o registro de ações médicas e à otimização dos atendimentos clínicos. Este instrumento é composto pelo conjunto de documentos padronizados, ordenados e concisos, destinados ao registro de todas as informações referentes aos cuidados médicos, paramédicos e laboratoriais prestados ao paciente.

A Resolução 1638/2002[111], do CFM, define o prontuário médico como “o documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada”. Ademais, a resolução indica que o prontuário médico tem como finalidade viabilizar a comunicação entre membros da equipe multiprofissional, visando a manutenção do tratamento integral e contínuo.

Constam nestes instrumentos todos os dados relativos ao paciente[112], como sua anamnese, histórico hospitalar, descrição e evolução de sintomas e exames, descrições de tratamentos e prescrições. Sendo composto por informações valiosas tanto para o paciente como para o próprio profissional da saúde, o que facilita o atendimento ao paciente.

Cabe destacar uma distinção terminológica inerente a esta questão. Apesar do termo utilizado ser” prontuário médico”, este documento é de propriedade do paciente. Isto faz com que o titular dos dados tenha total direito de acesso e poder de solicitação de cópia ou retificação, assim, ao estabelecimento de saúde e à equipe multidisciplinar que atua no caso cabe, pois, a sua elaboração e guarda.

Nesse sentido, respaldando a propriedade do prontuário ao paciente, tem-se o Recurso Extraordinário 1.375.558 Acre[113], com a relatoria da Ministra Rosa Weber. No qual foi manejado recurso extraordinário pelo Ministério Público do Estado contra o acórdão prolatado pelo Tribunal de Justiça do Estado do Acre. Na minuta, o recorrente assevera ter,

---

[111]CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 1.638, de 10 de julho de 2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde Brasília: CFM, 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 01 dez. 2023.

[112]FARINA, Arnaldo. Prontuário Médico. **Portal CFM**, 1999. Disponível em: https://portal.cfm.org.br/artigos/prontuario-medico/. Acesso em: 05 jan. 2024.

[113] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1375558/AC.** Direito Constitucional. Prontuários médicos de pacientes atendidos na rede pública estadual. Documento de natureza sigilosa. Requisição direta pelo Ministério Público do Estado para fins de investigação criminal. Impossibilidade. Reserva de Jurisdição. Direito à Intimidade. Recurso Extraordinário a que se nega seguimento. Relatora: Min. Rosa Weber, 02 set. 2022. Diário de Justiça, nº 179, divulgado em 08 set. 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6373575. Acesso em: 05 dez 2023.

constitucionalmente (art. 129, VI, da CF/1988), “direito de acesso a informações sigilosas documentadas em prontuários médicos”. Diante desse cenário a Ministra expõe:

> […] Como assentado na origem, o prontuário reúne dados referentes aos procedimentos, exames, condições físicas e outras informações particulares do paciente, cujo sigilo se impõe ao médico como exigência ética de sua conduta (arts. 73 e 89 do Código Ética Médica), ressalvadas as hipóteses em que haja de autorização do paciente para divulgação, requisição judicial ou a utilização do documento como meio de defesa do profissional.
> [...] Por essa razão, consignou o Min. Gilmar Mendes, redator designado para o RE nº 593.727 (Tema nº 184): "Em síntese, reafirmo que é legítimo o exercício do poder de investigar por parte do Ministério Público, porém essa atuação não pode ser exercida de forma ampla e irrestrita, sem qualquer controle, sob pena de agredir, inevitavelmente, direitos fundamentais. A atividade de investigação, seja ela exercida pela Polícia ou pelo Ministério Público, merece, por sua própria natureza, vigilância e controle".
> [...] Assim, o art. 129, VI, da Constituição não franqueia ao Ministério Público, sem prévia autorização judicial, acesso a documento protegido por sigilo, como são os prontuários médicos, em jogo restrição ao direito fundamental à intimidade.

2.2.1 Vantagens e desvantagens da utilização do prontuário digital

O instrumento em questão passou por significativas transformações com o advento dos avanços tecnológicos, tornando-se conhecido como PEP (Prontuário Eletrônico do Paciente) e é um dos documentos mais utilizados na rotina médica das clínicas modernizadas.

Diferente do prontuário de papel, o PEP auxilia nos processos organizacionais existentes e facilita a resolução da questão de saúde apresentada, posto não só a pronta apresentação de um vasto histórico hospitalar do paciente, equipado com dados de múltiplos profissionais, como também uma gama significativa de prescrições e protocolos adotados. Inclusive, a Resolução do CFM nº 2.056/2013[114] reitera a necessidade de registro integral das condutas no prontuário médico.

A implementação do prontuário médico eletrônico ocorreu com base na Resolução 1.821/2007[115] do CFM, a qual aprovou normas técnicas para a digitalização e uso de

---

[114] CONSELHO FEDERAL DE MEDICINA (CFM). Fiscalização: CFM estabelece regras mínimas para serviços de assistência médica. **Portal CFM**, Brasília, 12 nov. 2013. Disponível em: https://portal.cfm.org.br/noticias/fiscalizacao-cfm-estabelece-regras-minimas-para-servicos-de-assistenciamedica/#:~:text=Registro%20de%20prontu%C3%A1rios%20%E2%80%93%20Os%20hospitais%20tamb%C3%A9m%20ter%C3%A3o,demais%20profissionais%20de%20sa%C3%BAde%20que%20intervenham%20na%20assist%C3%AAncia. Acesso em: 01 jan. 2024.

[115] CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 2. 218, de 29 de novembro de 2018**. Revoga o artigo 10º da Resolução CFM nº 1.821/2007, de 23 de novembro de 2007. Brasília: CFM, 2018.

sistemas informatizados para guarda e manuseio de prontuários, autorizando a eliminação do papel na elaboração dos prontuários.

A Resolução supramencionada estabeleceu que o prontuário físico deve ser arquivado por, no mínimo, 20 anos a partir do último registro, prazo que foi mantido pela legislação atual. Esta que, por sua vez, estabeleceu mesmo prazo de armazenamento para o prontuário digital.

O documento também estabeleceu que o CFM e a Sociedade Brasileira de Informática em Saúde (SBIS) expediriam selo de qualidade dos sistemas, o que fora posteriormente revogado pela Resolução nº 2.218/2018 do próprio CFM[116]. Ante a necessidade de um estudo atual mais pormenorizado, revendo as regras para assinatura de novo convênio, trazendo maior segurança operacional aos prontuários eletrônicos que reúna dados adequados a nova realidade tecnológica.

O processo de digitalização, *lato sensu*, ganhou contornos relevantes com a lei 13.787/18[117], a qual dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário do paciente.

A normativa em questão determinou que o processo de digitalização deveria utilizar certificado digital baseado nas diretrizes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Esta que representa[118] “uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão”.

Essa tutela e busca pela adequada segurança do prontuário reside não apenas na mencionada necessidade de salvaguardar as informações sensíveis dos pacientes de falhas no armazenamento dos dados, mas também os proteger contra ingerências externas cada vez mais frequentes, as quais serão aprofundadas posteriormente.

Para a presente abordagem, urge pontuar que apesar dos riscos inerentes ao armazenamento dos prontuários em *software* médico, esta opção apresenta inúmeras

---

Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2218. Acesso em: 01 jan. 2024.

[116] CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 2. 218, de 29 de novembro de 2018**. Revoga o artigo 10º da Resolução CFM nº 1.821/2007, de 23 de novembro de 2007. Brasília: CFM, 2018. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2218. Acesso em: 01 jan. 2024.

[117] BRASIL. **Lei n. 13.787, de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 01 jan. 2024.

[118] BRASIL. Instituto Nacional de Tecnologia da Informação. ICP-Brasil. **Gov.br**, 2023. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em: 01 jan. 2024.

vantagens. A exemplo da otimização das atividades, já que por meio do PEP, pode-se agilizar o atendimento e permitir uma atenção muito maior frente às demandas do paciente.

Outrossim, cabe mencionar o aspecto da acessibilidade. Já que, no âmbito virtual, o acesso é instantâneo através de aparato conectado à rede. Respeitando a diretriz emitida pelo CFM, segundo a qual os dados do prontuário devem estar constantemente disponíveis, "de modo que, quando solicitado por ele - o paciente - ou seu representante legal, permitam o fornecimento de cópias autênticas das informações"[119].

Para além das disposições expostas, cabe ressaltar a integração dos dados dos pacientes realizada pela dinâmica trazida pelo arquivo eletrônico. Assim, além de diminuir as chances de extravio de dados, essa centralização poupa o tempo que seria gasto repetindo as mesmas perguntas de atendimentos anteriores ou consultando dezenas de arquivos.

Ressaltando, mais a economia dos espaços que antes eram usados para guardar pilhas de prontuários de papéis e agora podem ser utilizados para outras atividades. Dentre outras vantagens que podem ser elencadas.

Contudo, cabe reiterar que apesar das inúmeras vantagens associadas ao uso do prontuário digital, existem riscos a ele atrelados, os quais devem ser mencionados para uma maior compreensão quanto ao necessário investimento nos aparatos de segurança destes dados.

2.2.2 Interesses e ameaças do ataque hacker

Antes de ingressar propriamente na esfera do risco, cabe mencionar que os mencionados dados, para além do exposto, atuam como fator vital para engrenagens da economia da informação, conforme dispõe Bioni[120]. Para exemplificar e caracterizar ainda mais a referida arguição tem-se o exemplo dado pelo autor da auto regulação da produção trazida pela era da economia informativa.

---

[119] CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 1.821, de 11 de julho de 2007**. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Brasília: CFM, 2007. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-cfm-no-1-821-de-11-de-julho-de-2007. Acesso em: 01 jan. 2024.

[120] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2019. Pág. 6-9.

Por meio da internet, os dados dos usuários da rede, bem como as interações por tais efetivadas atuam como fortes reguladores de mercado. Exemplos evidenciam-se com a mutação da oferta por meio do compartilhamento e troca de experiências, em tempo real, dos usuários que consomem as informações veiculadas nos canais em questão. Assim, a informação produzida por quem utiliza as redes gera um próprio movimento de consumo.

Fica evidente, portanto, a relevância das informações pessoais em comento, sendo, o gerenciamento de tais um elemento extremamente estratégico para os negócios na atualidade. Gerando, cada vez mais, o interesse das empresas e setores nessa matéria, especialmente quanto a tratamento envolve dados sensíveis.

Trazendo para a perspectiva do atendimento médico-hospitalar, no qual os dados veiculados nessa relação, como já devidamente explanado, são sensíveis e abordam questões extremamente íntimas, cabe analisar alguns dos possíveis interessados na aquisição dessa informação. Os quais justificariam uma maior cautela dos agentes que realizam o tratamento destes dados.

Ab initio, é oportuno fazer um recorte desta análise para a vertente puramente comercial da aquisição dessa informação. Ora, para além do uso dos dados em comento para personalização de um bem a ser ofertado, cabe perceber a possibilidade do uso de tais para fins da publicidade direcionada de produtos que já existem no mercado.

Nesse diapasão, Bioni[121] aponta que tal forma persuasiva de apresentar o produto ao consumidor de modo direcionado é uma prática que acrescenta determinado fator a relação encomenda o qual incrementar a possibilidade de êxito na indução ao consumo promovendo uma comunicação certeira qual aquele público-alvo.

Desse modo, sendo tais dados tidos como peças singulares dessa engrenagem, estes podem ser utilizados e aplicados na efetivação da venda aos titulares dos dados interceptados[122]. Estes que, por sua vez, são pessoas que, no vertente caso, estão ainda mais vulneráveis em decorrência da própria condição de saúde.

Nesse sentido, a vulnerabilidade inerente do consumidor da relação contratual em tela, principalmente no que concerne à publicidade direcionada, acentuasse ainda mais conforme o caso concreto. Nas situações mais simples, os reflexos da indução do paciente

---

[121] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2019. p. 20.

[122] RÊGO, Isabelle Souza Ulisses. **Telemedicina**: análise sobre a responsabilidade civil do terceiro no tratamento indevido de dados sensíveis do paciente. 2021. 73f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Piauí, Teresina, 2021.

à aquisição de um produto acabam sendo relativamente mitigados, contudo, nos casos mais graves, o paciente está submetido a uma vulnerabilidade maior ante a necessidade de aquisição urgente daquele produto.

Exemplos evidenciam-se com a busca por tratamentos estéticos de maneira virtual e o aparecimento de informações que remetam a solução do problema abordado por meio da aquisição de determinada marca existente no mercado. Ou, em casos mais graves, quando o paciente, a título exemplificativo, adquire o coronavírus e busca, virtualmente, a solução para alguns sintomas classificados como significativamente graves. Esse problema encontra escopo, assim, nas resoluções de situações de saúde apresentadas por terceiros que obtiveram, de forma inapropriada, aquele dado sensível.

Essa vertente apresentada é apenas uma das possíveis formas da utilização indevida dos dados veiculados na consulta. Existindo, inclusive, uma modalidade ainda mais gravosa que é a possibilidade de determinada empresa, por exemplo, invadir de forma ilícita o sistema e alterar o prontuário para o acréscimo ou modificação de marca específica de medicamentos ou de utensílios vinculados ao tratamento do paciente. Induzindo-o, assim, a adquirir aquele produto. O levando, inclusive, a acreditar que fora por recomendação médica.

Um dado médico de um paciente vazado, por exemplo, a um plano de saúde pode vir a ocasionar um reajuste do tabelamento de valores a ele apresentado. Gerando uma oneração dos custos atrelados à prestação do serviço.

E as hipóteses não se esgotam nas estruturas apresentadas. Por se tratarem de dados especialmente sensíveis, como os de saúde, existe um desejo ainda mais acentuado de cerca-los sob o âmbito privado do indivíduo, já que são dados passíveis de uso discriminatório. Assim, existe a possibilidade de hackers invadirem o sistema, absorverem os dados e os utilizarem como instrumento de chantagem ao paciente em troca de determinado valor pecuniário.

Nesse sentido, cabe mencionar mais um risco de natureza extremamente grave, cuja conjuntura fática se materializou recentemente. No qual, um grupo de cibercriminosos sequestrou e divulgou “imagens íntimas e dados financeiros de pacientes de um consultório

de cirurgia plástica do Rio Grande do Sul e do Paraná”[123]. Os danos inerentes à vertente exposição atingem proporções significativas, as quais dariam vasta discussão.

A publicação em questão, segundo a mídia, fora materializada pelo grupo Qiulong na *deep web* e constou de um pedido de resgate visando a não divulgar do resto dos dados nas redes sociais. A ação da organização foi identificada pela empresa ISH Tecnologia no dia 22 de abril de 2024.

Este incidente destaca a sofisticação e a audácia crescentes de ataques *ransomware* no setor da saúde, um dos setores mais visados por esse tipo de crime no Brasil. Trazendo mais uma relevante preocupação quanto a salvaguarda adequada dos sistemas de armazenamento de dados.

A disponibilização irregular na *deep web* alcança, também, danos à própria instituição hospitalar. Um exemplo prático, fora o ataque de *hackers* que afetou o sistema do Hospital de Câncer de Barretos, em junho de 2017, e prejudicou a realização de ao menos 350 exames, conforme dispõe o jornal A Folha Digital[124]. Ocasionando uma gama considerável de danos aos envolvidos, quer seja o hospital ou os pacientes, em especial os que não puderam ser atendidos.

No caso em apreço, o resgate requerido pelos criminosos, que contaminaram a rede com um tipo *ransomware* , era de US$ 300 por máquina[125]. Ocasionando um custo de US$ 360 mil ao nosocômio, o equivalente a R$ 1,08 milhão. Em uma análise do caso, Perrotti delineou que além do custo financeiro, houve o custo humano.

Segundo o autor, cerca de 3 mil consultas e exames foram cancelados e 350 pacientes ficaram sem radioterapia por conta da invasão. Ademais, coube acrescentar que outras unidades do hospital, as quais estavam localizadas em Jales (SP) e Porto Velho (RO), também haviam sido afetadas.

---

[123] O GLOBO. **Ameaças e pedidos de resgate: Hackers vazam imagens de pacientes nus de clínica de cirurgia plástica do Sul.** 2024. Disponível em: https://oglobo.globo.com/brasil/noticia/2024/04/29/hackers-vazam-imagens-de-pacientes-nus-de-clinica-de-cirurgia-plastica-do-sul-e-prontuarios-de-saude-sexual.ghtml. Acesso em: 07 maio 2024.

[124] TOLEDO, Mônica. Hackers invadem sistema do Hospital de Câncer de Barretos e pedem resgate. **Folha de São Paulo**. 2017. Disponível em: https://www1.folha.uol.com.br/cotidiano/2017/06/1896638-hackers-invadem-sistema-do-hospital-de-cancer-de-barretos-e-pedem-resgate.shtml. Acesso em: 26 dez. 2023.

[125] PERROTTI, Paulo. Saúde: clínicas são as que mais sofrem com ataques cibernéticos. **Solution Hub**. 2023. Disponível em: https://solutionhub.com.br/saude-clinicas-sao-as-que-mais-sofrem-com-ataques-ciberneticos/. Acesso em: 18 abr. 2024.

Ademais, cabe mencionar o recente ataque *hacker* ao INCA[126], Instituto Nacional do Câncer, o órgão auxiliar do Ministério da Saúde no desenvolvimento e coordenação das ações integradas para a prevenção e o controle do câncer no Brasil. A situação tomou proporções significas, de modo que as sessões de radioterapia foram suspensas por causa do ataque no dia 27/01/2024. A paralisação em questão afetou pelo menos 100 pessoas. Evidenciando a ocorrência de danos que transcendem à própria prestação do serviço.

Outrossim, o Hospital Universitário da USP confirmou, em comunicado enviado à Security Report[127], a ocorrência de uma invasão por hacker aos sistemas informatizados no dia 30/03/2023. A Instituição precisou restringir os atendimentos aos casos emergenciais e urgentes.

Para além dos graves ataques relatados, em novembro de 2021, *Hackers* invadiram e criptografaram os sistemas do Instituto de Gestão Estratégica de Saúde do Distrito Federal[128], IGESDF, o qual administra os principais hospitais públicos da capital.

Essa questão já vem sendo discutida[129] há alguns anos pelo canal virtual The State of Security[130], o qual dispôs sobre algumas modalidades de ataques cibernéticos (*cyber-attacks*). Em recente manifestação[131], dispuseram que em meio à pandemia que oprime a

---

[126] COUTINHO, Rogério. Inca cancela consultas e exames após sistema sofrer invasão hacker; não há previsão de retorno. **Globo**, 2024. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/01/29/sistema-do-inca-sofre-invasao-hacker.ghtml. Acesso em: 26 mar. 2024.

[127][127] SECURITYLEADERS. **Hospital Universitário da USP confirma ataque hacker aos sistemas informatizados**. Disponível em: https://securityleaders.com.br/hospital-universitario-da-usp-confirma-ataque-hacker-aos-sistemas-informatizados-2/ Acesso em: 08 mar. 2024.

[128] OBASTIDOR. **Hackers invadem sistemas de hospitais públicos de Brasília**. https://obastidor.com.br/investigacao/hackers-invadem-sistemas-de-hospitais-publicos-de-brasilia-2119. Acesso em: 08 mar. 2024.

[129] "Predators usually single out the slow and weak to attack. If these hackers can steal a medical account, they can quickly sell that number to black marketers for a price up to ten times more than that of a stolen credit card. Then the black marketers buy the account number to purchase medical supplies and drugs. Some enterprising black marketers will also create authentic looking medical cards to sell to the truly desperate who will use it to go to a clinic, dentist, chain store optometrist or even to seek critical care at an emergency room. The stolen medical accounts stay valid for months until legitimate patients start getting invoices. Medical companies have needed little fraud detection and therefore their detection and recovery instincts are not yet up to the challenge. Yet, solutions to reduce medical account fraud are technically straightforward. Simply demonetize the value of stolen medical account numbers by requiring two factor authentication prior to authorizing care delivery. Unfortunately, cyber security solutions are rarely, if ever, purely technical".

[130] TRIPWIRE. **Why Hackers Are After The Healthcare Industry**. 2015. Disponível em: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/why-anthem-why-now/. Acesso em: 26 dez. 2023.

[131] ARAMPATZIS, Anastasios. Cibersegurança e conformidade para organizações da saúde. **Tripwire**, 2021. Disponível em: https://www.tripwire.com/state-of-security/healthcare/cybersecurity-and-compliance-for-healthcare-organizations/. Acesso em: 26 dez. 2023.

capacidade de muitos sistemas hospitalares, os *hackers* mal-intencionados têm sido rápidos em atacar os provedores de saúde e agências médicas.

Hospitais e organizações de saúde eram alvos atraentes mesmo antes da pandemia do coronavírus. Os registros dos pacientes têm quase tudo que um invasor precisa em um único documento para realizar esquemas sofisticados de fraude em seguros, comprar suprimentos médicos ou medicamentos ou mesmo cometer outros tipos de fraude, incluindo roubo de identidade total. Os registros médicos, portanto, são alvos lucrativos e ativos caros no submundo do crime cibernético.

Além disso, através dos ataques, os agentes podem roubar propriedade intelectual[132], dados de pesquisa, informações quanto a testes de medicamentos, registros médicos e similares. Tais dados de investigação roubados, muitas vezes representam um investimento financeiro significativo, o qual vincula-se a anos de investigação e ensaios dispendiosos em pacientes. Trazendo mais uma relevante preocupação quanto a salvaguarda adequada dos sistemas de armazenamento de dados.

Para além das hipóteses supramencionadas, urge pontuar que a visibilidade inerente aos prestadores de cuidados de saúde[133], como clínicas e hospitais, é de extrema notoriedade. Os tornando ainda mais atraentes pelo grande impacto que podem ocasionar, atuando, por si só, como um motivador chave para a atuação dos setores mal-intencionados.

Exemplo evidencia-se com a utilização do *ransomware* pelos invasores, o que pode afetar gravemente as operações diárias dos prestadores de cuidados de saúde. Nessa modalidade, utiliza-se um tipo de malware[134] que sequestra os dados de uma organização, podendo paralisar as operações de uma empresa, interrompendo o acesso a sistemas críticos e aplicativos. Indo além, os ataques disruptivos podem desativar, sabotar ou deletar dados em sistemas críticos[135] dentro de um hospital.

---

[132] FUENTES, Maricel Rivera; HUQ, Nashid. **Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf. Acesso em: 26 abr. 2024.

[133] *Ibid.*

[134] Termo genérico associado a qualquer tipo de *software* malicioso, especialmente projetado para prejudicar ou explorar dispositivos virtuais.

[135] Setores ligados a alas de urgência e emergência ou pronto atendimento.

Ademais, casos recentes de invasões podem ser mencionados. A exemplo dos hospitais administrados pela empresa Prospect Medical Holdings[136], os quais tiveram, em agosto de 2023, os seus serviços paralisados em vários estados dos Estados Unidos após um ataque cibernético.

Esses ataques continuaram atingindo os Estados Unidos e a Europa nos últimos meses, servindo como um lembrete para as organizações revisarem de perto sua postura de segurança da informação durante esses tempos de incerteza.

A implantação de novos dispositivos, especialmente aqueles que usam redes sem fio e sensores para coletar e trocar informações, é uma faca de dois gumes. Embora esses dispositivos ofereçam aos ambientes médicos recursos incríveis para cuidar de pacientes e aumentar a eficiência do atendimento, cada dispositivo aumenta a superfície de ataque de uma organização.

Portanto, a produção de estratégias normativas e, principalmente, de responsabilização dos agentes irregularmente interventores devem ser significativamente perseguidas e ampliadas. Haja vista que atuam não só como instrumentos de salvaguarda das mencionadas prerrogativas constitucionais e da liberdade deliberativa do paciente, mas também como um dos princípios norteadores da relação profissional em questão.

Cabendo ressaltar que, no vertente caso, o paciente é vulnerável, por se tratar de dados de natureza personalíssima e potencialmente discriminatória. Assim, a existência das mencionadas garantias teria o condão de assegurar a autonomia do paciente de transmitir os seus dados sensíveis apenas para o profissional que lhe assiste, tendo o direito pessoal de impedir o acesso e a divulgação indevidos de terceiros às informações pessoais ali disponibilizadas.

Nesse diapasão, evidencia-se com notória nitidez que essas protetivas correm riscos consideráveis nas relações mediadas pela tecnologia. Em conformidade com o outrora exposto, com o advento do desenvolvimento de novos recursos tecnológicos, não se pode falar ainda em confiabilidade absoluta, em rede, na preservação de dados pessoais de natureza sensível, mesmo considerando a exigência crescente de aplicação das melhores técnicas de segurança.

---

[136] ASSOCIATED PRESS. Ataque hacker interrompe funcionamento de hospitais nos Estados Unidos e FBI abre investigação. **Globo**, 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/08/10/ataque-hacker-interrompe-funcionamento-de-hospitais-nos-estados-unidos-e-fbi-abre-investigacao.ghtml. Acesso em: 05 jan. 2024.

Portanto, os dados obtidos durante uma consulta devem ser protegidos para evitar acesso de terceiros não autorizados. Desse modo, caso o hospital adote determinada plataforma de atendimento, este deverá analisar se esta possui uma política de privacidade adequada que abarque um conjunto de medidas de segurança apropriadas e constantemente atualizadas.

2.3 DEVERES EXTRACONTRATUAIS DO HOSPITAL E A PROTEÇÃO DE DADOS DOS PACIENTES. BREVÍSSIMAS ANOTAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NA SAÚDE DIGITAL

Diante do exposto, tendo em vista as questões trazidas, o legislador verificou que as estruturas normativas existentes não eram suficientes para salvaguardar a tutela destes dispositivos. Fenômeno este decorrente da existência de, tão somente, códigos vigentes que pouco dispunham sobre essa abordagem e de espaças estruturas regulamentadoras como, por exemplo, o Marco Civil da internet.

Ora, conforme o doutrinador Bruno Bioni[137] até a aprovação da LGPD, o Brasil contava uma verdadeira “colcha de retalhos” que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia sequer uniformidade em seu regramento. De modo que:

> Essa assimetria gerava insegurança para: a) que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios; b) a formulação de políticas públicas e parcerias público-privadas igualmente dependentes desse intercâmbio de dados; e c) o cidadão que não detinha uma proteção integral e universal com relação a todas as atividades do cotidiano em que fornece seus dados, seja para o setor privado ou público. Sendo a proteção do consumidor e a dignidade da pessoa humana erigidas como princípios da ordem econômica pela Constituição Federal (art. 170, caput e inciso V, da Constituição Federal) que conformam a livre-iniciativa281, mostra-se ainda mais pertinente o diagnóstico dessa dupla faceta de leis gerais de proteção de dados pessoais, especialmente para se cumprir com o que foi programado em termos de ordem econômica pelo texto constitucional.

[137] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 103.

Assim, conforme orientam Tepedino e Spadaccini, o desenvolvimento[138] de mecanismos destinados a regular o tratamento dos dados é fundamental, pois auxilia a evitar discriminações que não encontrem fundamento constitucional. Ademais, tais estruturas evitam a ocorrência de práticas que possam prejudicar a liberdade dos indivíduos, ou afetem de modo negativo a vida desses particulares cujos dados são tratados, evitando a ampliação de assimetrias, preconceitos e desigualdades.

Partindo desse pressuposto, o legislador brasileiro, por meio da Lei Geral de Proteção de Dados, busca estratégias de salvaguarda normativa dessas estruturas tão basilares para a formação da personalidade e da sociabilização do indivíduo. Estas que, por seu turno, estão cada vez mais visadas, frente ao processo constante de mercantilização dos dados.

Ademais, este aparato protetivo procurou tecer uma norma neutra tecnológica, posto que, adequadamente, deixou de apontar uma tecnologia em específico que poderia se tornar obsoleta ao longo do tempo.

Cabendo ressaltar que também se utilizara de alguns conceitos indeterminados, a exemplo da noção de razoabilidade. Simultaneamente, contudo, prescreveu balizas para reduzir a discricionariedade de tal exercício interpretativo e, com isso, alcançar um mínimo de previsibilidade quando tal norma viesse a ser colocada em movimento.

Passado o exposto, e para uma melhor compreensão das seguintes disposições sobre a norma supra, urge delinear sobre alguns conceitos que são basilares para esse dispositivo. Quais sejam: a ideia de tratamento, de controlador e de operador[139].

Para os fins legais, tratamento é tido como toda operação realizada com dados pessoais, ou seja, as mais variadas utilizações destes estão abarcadas nesse conceito, quer seja a coleta, acesso, reprodução, transferência, dentre outras possibilidades.

Ao passo que a noção de controlador se vincula à pessoa, quer seja natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Para a vertente pesquisa, o hospital assume esse papel de

---

[138] TEPEDINO, Gustavo. **Novos princípios contratuais e a teoria da confiança: a exegese da cláusula to thebest knowledge of the sellers**. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5600369/mod_resource/content/1/Novos%20Princ%C3%ADpios%20Contratuais%20e%20Teoria%20da%20Confian%C3%A7a%20a%20exegese%20da%20cl%C3%A1usula%20to%20the%20best%20knowledge%20of%20the%20sellers%20-%20Gustavo%20Tepedino%20.pdf. Acesso em: 28 jun. 2021.

[139] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

controlador dos dados dos pacientes. Outrossim, compete ao denominado operador a realização propriamente do tratamento em nome do controlador.

Passados os esclarecimentos quanto aos conceitos supra, cabe analisar, para além do aparato regulatório aqui utilizado, quais são os requisitos mínimos os quais devem ser atendidos para que o tratamento dos dados não esteja eivado de vícios. Por certo, adotar-se-á, principalmente, a perspectiva da relação hospital- paciente a qual é objeto da vertente análise.

Requisitos estes que, por sua vez, serão fundamentais para a subsequente disposição quanto à responsabilização dos envolvidos no incumprimento das estruturas normativas que tutelam as protetivas constitucionais em comento. Introduzindo-se tal abordagem por meio de sucinta disposição quanto ao consentimento do titular dos dados.

2.3.1 Deveres impostos pela LGPD ao controlador pelo tratamento de dados

A normativa que regulamenta a proteção de dados estabelece uma série de obrigações e responsabilidades para as empresas e profissionais que utilizem, em alguma medida, tais dados para a prestação dos seus serviços ou fornecimento dos seus produtos. No setor de saúde[140], onde a coleta, armazenamento e uso de dados é essencial para a prestação de serviços médicos, essa legislação tem implicações significativas.

Inicialmente, a LGPD orienta em seu bojo que devem ser observados no tratamento dos dados a boa-fé e princípios[141] como a finalidade, segundo a qual tais informações devem ser utilizadas para propósitos legítimos, específicos, explícitos, bem como devem ser informados ao titular. Inclusive, nesse interim, a normativa ainda acrescenta a impossibilidade de tratamento posterior de forma incompatível com os propósitos notificados ao titular, em respeito, inclusive, às disposições atrás mencionadas quanto ao consentimento esclarecido.

---

[140] SILVA. Ernesto Tavares da. A responsabilidade do profissional da saúde na proteção dos dados pessoais de pacientes, de acordo com a LGPD. **Migalhas**, 28 mar 2023. Disponível em:https://www.migalhas.com.br/amp/depeso/383751/profissional-da-saude-e-a-protecao-dos-dados-pessoais-de-pacientes. Acesso em: 09 dez. 2023.

[141] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

A coleta de dados pessoais, também, deve ser limitada ao mínimo necessário para o tratamento do paciente[142], conforme preceitua o princípio da necessidade expressamente previsto na normativa infraconstitucional supramencionada. Ressaltando, também, a estrutura principiológica fincada na realização do tratamento segundo a finalidade legítima, específica, explícita e informada ao titular. Assim como, a qualidade destas informações deve ser assegurada, esta que, por sua vez, é tida nas vertentes da clareza, da exatidão e da atualização.

Ademais, tem-se a transparência, ressalvados os segredos comerciais e industriais, a segurança e a prevenção, enquanto utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados das situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão e a não discriminação.

Os dados pessoais tratados são armazenados pelo tempo estritamente necessário para atingir a finalidade informada ao titular, após o seu decurso, tais dados pessoais poderão ser mantidos para o cumprimento de obrigação legal e uso exclusivo das referidas Instituições.

Dentro do rol de responsabilidades do controlador, cabe a menção ao dever de informar os pacientes sobre como seus dados serão tratados[143], dispondo sobre seus direitos. A exemplo da prerrogativa de acesso, retificação, exclusão e portabilidade, bem como de receber uma cópia desses dados em um formato legível por máquina. Cabendo, mais, informações sobre a confirmação da existência de tratamento, as quais devem ser claras e objetivas, em linguagem acessível e de fácil compreensão. Informando, inclusive, sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Urge mencionar que a LGPD também dispõe quanto a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei[144].

A norma supramencionada elucida, mais, que devem ser asseguradas a responsabilização e prestação de contas, de modo que ocorra a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o

---

[142] *Ibid.*
[143] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.
[144] *Ibid.*

cumprimento das normas de proteção de dados pessoais. Requerendo, inclusive, a comprovação da eficácia dessas medidas.

Além do outrora exposto, a norma dispõe[145], em seção específica, sobre questões relevantes que precisam ser observadas por quem gerencia esses dados. Dentre as quais: a manutenção do registro das operações de tratamento das informações que realizarem, bem como, caso a autoridade nacional determine, a elaboração de um relatório[146] do impacto à proteção de dados pessoais, observados os segredos comercial e industrial.

Outrossim, ainda enquanto uma preocupação do legislador no estabelecimento de deveres aos agentes de dados, tem-se a disposição sobre o que seria uma atuação irregular[147]. Conforme expressa conjuntura do artigo 44 da protetiva em comento, quando o profissional deixar de observar a legislação ou quando não fornecer a segurança que o titular de boa-fé dele pode esperar incorrerá na presente irregularidade.

Cabendo ressaltar que essa expectativa se finca não apenas nas protetivas principiológicas trazidas no início da presente disposição, como também nas informações repassadas com o fito de obtenção do consentimento. Ora, tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas de modo que, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade.

Nesse diapasão, a norma prevê a análise de determinadas circunstâncias que interferem nessa relação como a forma utilizada, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Bem como, por meio do parágrafo único do artigo em comento, reitera quanto a responsabilidade do controlador ou do operador pelos danos decorrentes da violação da segurança dos dados ao deixar de adotar as medidas de segurança previstas, dando causa ao dano.

Seguindo este mesmo fito indenizatório, o artigo 42 impõe o dever de indenizar ao controlador ou operador que causar danos ao titular de dados, pelo exercício de sua

---

[145] *Ibid.*

[146] Embasado nas operações de tratamento de dados realizada. O aparato em comento, conforme critérios legais, deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

[147] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

atividade. Ficando evidente o seu intento de balizar a indenização na ocorrência do dano, quer seja moral, material ou coletivo, e com a tão somente configuração do nexo causal e da demonstração do dano.

A LGPD estabeleceu, de forma similar ao Código de Defesa do Consumidor, CDC, a solidariedade dos agentes de tratamento que causarem lesão[148] e permitiu a inversão do ônus da prova por critério judicial para mitigar a assimetria na relação entre controladores, operadores e titulares de dados pessoais. Assegurando, em sequência, o direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Contudo, o tratamento da responsabilidade civil no âmbito da LGPD tem sido tema de diversos debates na doutrina moderna a respeito, principalmente, da natureza da obrigação de indenizar. Podendo ser subjetiva, a qual se sustenta na ausência do cumprimento de um dever de conduta imposto ao agente de tratamento, ou objetiva, sendo esta fundamentada no risco da atividade desenvolvida pelos agentes, conforme pontua[149] a doutora Caitlin Mulholland[150].

Nessa mesma linha, Tasso[151] reitera que há uma imprecisão normativa quanto ao sistema de responsabilidade civil adotado pela LGPD, pois o enunciado do art. 42 não teria sido suficientemente claro quanto ao regime de responsabilidade civil adotado pela norma. Ora, mesmo que tal dispositivo não faça referência expressa à culpa como elemento da responsabilidade civil, este também não faz qualquer alusão ao risco como fundamento claro para a configuração da responsabilidade objetiva.

2.3.2 Deveres do hospital e boas práticas em segurança de dados

---

[148] *Ibid.*

[149] ROSENVALD, Nelson; CORREIA, Anderson; MONTEIRO FILHO, Carlos Eduardo do Rêgo; KHOURI, Paulo Roberto. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em: 26 dez. 2021.

[150] MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *In:* MARTINS, G. M.; ROSENVALD, N. (Org.). **Responsabilidade civil e novas tecnologias**. 1ed. Belo Horizonte: Editora Foco, 2020, v. 1, p. 109-124. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 06 dez 2023.

[151] TASSO, Francisco Augusto. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

Para além dos deveres inerentes à legislação de proteção de dados, alguns standards de segurança devem ser observados para que se fale propriamente em uma adequada prestação do serviço de gestão dos dados sensíveis dos pacientes. Por certo, cabe ressaltar que não existe um sistema ou estrutura conectada em rede que se afirme totalmente segura.

A falácia na proteção total de um sistema esbarra no próprio processo contínuo de evolução tecnológica. Inclusive, existe um conceito que adequadamente conversa com essa progressão digital que é o de ataques de dia zero. Nestes os hackers aproveitam falhas de software que os desenvolvedores desconhecem para atacar as vítimas sem aviso prévio.

Esta é uma falha de segurança de *software* recém-descoberta que não foi corrigida[152], porque continua desconhecida para os desenvolvedores do *software*. Os desenvolvedores descobrem quanto ao surgimento dessa "vulnerabilidade de dia zero" apenas depois que tal ataque acontece, não tendo, pois, aviso prévio para corrigir a vulnerabilidade antes da ocorrência do ataque.

O ataque pode ser realizado de diversas formas, dentre as quais o uso do chamado *fuzzing*[153]. Este mecanismo envolve a inserção de muitos dados no sistema, em intervalos distintos, acompanhada da análise de como o programa responde. Essa sobrecarrega dos programas pode fazê-los travar, o que pode resultar em um comportamento inesperado. A questão acaba sendo agravada quando as vulnerabilidades de dia zero são negociadas e vendidas entre hackers na *dark web*. O que amplia a possibilidade de ataque a um sistema.

Todos esses aspectos são relevantes para uma adequada discussão sobre a responsabilidade civil dos controladores de dados. A escolha dos protocolos mais atuais e a adoção de boas práticas em termos de segurança de dados pode garantir níveis de proteção mais altos, possibilitando, como analisaremos posteriormente, a interferência nas questões inerentes ao processo de responsabilização.

Dentre os principais standards de segurança, cabem algumas menções específicas a estratégias básicas no campo da computação quanto à proteção de dados. Exemplos evidenciam-se com a adoção da criptografia e da autenticação em camadas, da adequada

---

[152] FREDA, André. O que é um ataque de dia zero? **Avast, 2021**. Disponível em: https://www.avast.com/pt-br/c-zero-day Acesso em: 05 jan. 2024.
[153] *Ibid.*

atualização de software, de *Backup* de Bancos de Dados, de práticas em engenharia social, do *Single Responsiblity Principle* (Princípio da responsabilidade única) e da Certificações específicas em saúde.

O primeiro pressuposto básico para a segurança do sistema é a adoção da criptografia, enquanto método que converte textos em códigos abstratos, os conhecidos "*ciphertexts*" ou textos cifrados. O propósito desse instrumento é ocultar dados sensíveis, impedindo que usuários não autorizados acessem e roubem as informações.

O uso desse método, por si só, não garante uma adequada tutela sistêmica, devendo, pois, adotá-lo sob a perspectiva do conceito de Segurança em Camadas. Para um adequado aprofundamento sobre a matéria, cabe uma compreensão superficial sobre as três camadas principais da criptografia.

A proteção dos dados em descanso[154], ou seja, uma criptografia associada ao disco rígido em que se encontram os dados é conhecida como camada "*At Rest*", no qual usa o padrão de criptografia avançada (AES). Protege os dados por meio da codificação durante o armazenamento, para que não sejam retirados ou afetados em caso de comprometimento do sistema.

Quando se transcende para uma segurança no transporte dos dados, gerando uma codificação em movimento. Fala-se em camada de criptografia em trânsito, a qual protege os dados caso a comunicação seja interceptada durante a transmissão dos dados entre um site e um provedor de nuvem ou entre dois serviços. A exemplo, do uso do o protocolo "*Transport Layer Security* (TLS) para criptografar dados em trânsito e garantir a segurança de transporte e as *Secure/Multipurpose Internet Mail Extensions* (S/MIME) para proteger mensagens de e-mail"[155].

Por último, a codificação dos dados entre Sistemas, os chamados processos no âmbito da computação, tem-se a criptografia a Nível Transeunte, o qual "protege os dados na memória contra comprometimento ou exfiltração de dados criptografando os dados durante o processamento".

O conhecimento dessas camadas deixa evidente a necessidade da adoção de várias perspectivas da criptografia dos dados, visando uma maior segurança da informação

[154]GOOGLE CLOUD. **Criptografia em trânsito.** 2024**.** Disponível em:https://cloud.google.com/docs/security/encryption-in-transit?hl=pt-br. Acesso em: 08 jan. 2024.
[155] *Ibid.*

veiculada. Garantido que caso uma camada seja violada, a outra resta intacta, preservando o dado veiculado.

Passa-se, assim, à análise da autenticação[156], enquanto pressuposto de boas práticas, esta que é conhecida como a comprovação do direito de acesso a determinada estrutura informacional. Este mecanismo também deve ser associado à segurança em camadas para que ocorra uma adequada tutela da informação armazenada.

A primeira camada é conhecida como "*Something you know*" e abarca a ideia de usuário e senha. Assim, só é possível o acesso a determinado dado por quem sabe o código. Nesse setor, existem diversos mecanismos e recomendações para a construção desse acesso. Por exemplo, a existência de uma senha forte, com diversos caracteres distintos. Isso para evitar grandes vazamentos de dados como o apresentado na seguinte jurisprudência[157]:

> APELAÇÕES CÍVEIS. DANOS MORAIS. DANOS MATERIAIS. DIVULGAÇÃO DE PRONTUÁRIO MÉDICO. HIV. **Dados médicos do autor disponibilizados ao público no site** (...) a **simples inserção de seu CPF e sua data de nascimento, informações essas de fácil acesso**. Ausência de senha de acesso que torna a informação, na prática, pública. O vazamento do prontuário médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante no ambiente de trabalho. A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexo causal entre a conduta e este dano e a ausência de culpa excludente da vítima (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade. Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. Danos morais configurados. Quantum indenizatório majorado. Danos materiais não configurados. Ausência de prova de nexo de causalidade entre a exposição dos dados médicos e a efetiva demissão do autor. Honorários advocatícios readequados. Recurso do autor parcialmente provido. Recurso do réu desprovido. TJ-SP - AC: 10168440320208260068 SP 1016844-03.2020.8.26.0068, Relator: Heloísa Martins Mimessi, Data de Julgamento: 05/07/2021, 5ª Câmara de Direito Público, Data de Publicação: 07/07/2021 (Grifo meu).

---

[156] INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM BRASIL). **Autenticação de camada de mensagem**. 2023. Disponível em: https://www.ibm.com/docs/pt-br/was-nd/8.5.5?topic=mechanism-message-layer-authentication. Acesso em: 08 jan. 2024.

[157] SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. 5ª Câmara de Direito Público**. Apelação Cível nº 10168440320208260068 SP**. Danos Morais. Danos Materiais. Divulgação De Prontuário Médico. Hiv. Relatora: Heloísa Martins Mimessi. 07 de julho de 2021. Disponível em:https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2097727220/inteiro-teor-2097727224. Acesso em: 11 nov 2023.

Uma camada subsequente de autenticação é a conhecida pela expressão: *“Something you have*”, a qual representa uma validação via SMS, E-mail, ou outras estruturas. Requer, pois, a posse de outro sistema para adequada validação do usuário. Ademais, tem-se também a camada “*Something you are*”, a qual abarca estruturas inerentes ao próprio titular do acesso. A exemplo do reconhecimento facial, da biometria, da leitura de retina, dentre outros mecanismos.

Para além do outrora exposto, tem-se também a necessidade de continua atualização do *software*, conhecido como um processo no meio da computação, que está sendo utilizado. Contudo, cabe ressaltar que essa progressão sistêmica demanda dois tipos de custo: o monetário e o de instabilidade.

Um sistema de alto padrão e seu continuo ajuste demandam investimentos vultuosos constantes. Porém, não bastasse esse fator, uma atualização às vezes gera uma certa instabilidade, não apenas no aspecto de compatibilização do que fora atualizado com os demais mecanismos externos a ele anteriormente anexados, como na própria adaptação dos usuários. Por isso, os investimentos nesse setor acabam demandando consideráveis ponderações.

Vale ressaltar que um software de alta qualidade auxilia na minimização do risco de um ataque de *ransomware* [158]. Este faz parte da família dos *malwares,* tidos como *softwares* maliciosos, que atuam criptografando os dados afetados, os deixando indisponíveis ao titular. Normalmente, a liberação dessas informações está associada ao pagamento de vultuosas quantias a nível de resgate.

Outrossim, urge mencionar quanto aos *backups*[159]. Tidos como mecanismos de armazenamento de dados em estruturas de suporte mais seguras para que possam ser recuperados em caso de problemas como panes, vírus ou erros humanos. Devem estar atrelados a periódicas realizações de testes de restauração para garantir a eficácia do processo, assegurando que os dados possam ser recuperados de modo mais rápido e eficiente.

---

[158] KASPERSKY. **Ransomware: definição, prevenção e remoção**. 2023. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 08 jan. 2024.

[159] FEEGOW. **O que é backup do sistema e como fazer o da sua clínica?** 2020. Disponível em: https://feegowclinic.com.br/backup-do-sistema-blog/. Acesso em: 08 jan. 2024.

Não pode faltar a análise da conhecida Engenharia Social[160], a qual está associada ao treinamento dos usuários do sistema, já que este é tão seguro quanto seu elo mais frágil. O treinamento adequado dos profissionais e demais usuários sobre a adequada utilização do sistema é primordial para evitar os denominados "*Phishing*".

Este representa uma prática predatória que visa ludibriar o usuário de modo a roubar dinheiro ou a sua identidade. Opera fazendo com que você revele informações pessoais, quer seja sobre os números de cartão de crédito, informações bancárias ou senhas. Normalmente, atua por meio de sites que fingem ser legítimos ou e-mails de grandes intuições. Portanto, evidencia-se que esse aspecto da segurança dos dados está mais atrelado a um risco interno, o que será posteriormente explorado para fins de responsabilização.

Ademais, existe como pressuposto básico na construção de um sistema o conceito de *Single Responsiblity Principle* ou Princípio da Responsabilidade Única[161]. Esse princípio declara que uma "classe" deve ser especializada em um único assunto e possuir apenas uma responsabilidade dentro do *software*, ou seja, esta deve ter uma única tarefa ou ação para executar.

Em outra disposição, o usuário do sistema deve ter acesso apenas aos dados estritamente necessários para a execução de suas funções. Trazendo para o ambiente médico-hospitalar, o médico deve ter tanto acesso ao sistema quanto ele precisar para acessar os dados dos pacientes a ele vinculados, bem como para fazer suas respectivas prescrições. O administrador deve ter apenas o contato sobre as informações inerentes às suas atividades. O paciente deve ter amplo acesso apenas aos seus dados e questões a ele pertinentes.

A adoção de categorias com uma vasta amplitude de acesso amplia os riscos inerentes ao acesso indevido aos dados disponibilizados no sistema correlato. A existência de classes com mais de uma responsabilidade, as chamadas "*God Class*", geram demasiados riscos em eventual invasão, posto que o *hacker* acaba tendo acesso a tudo.

---

[160] KASPERSKY. **O que é engenharia social?** 2023. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 08 jan. 2024.

[161] WISKY, Daniel. SOLID. Princípio da Responsabilidade Única. **Blog Daniel Wisky**, 2023. Disponível em: https://danielwisky.com.br/2023-08-05-principio-responsabilidade-unica/#:~:text=O%20Princ%C3%ADpio%20da%20Responsabilidade%20%C3%9Anica,e%20a%20extensibilidade%20do%20c%C3%B3digo. Acesso em: 08 jan. 2024.

Por fim, para além do protocolo geral de proteção de dados, as informações sensíveis vinculadas à saúde possuem requisitos extra com a necessidade de certificados específicos, a exemplo dos S-RES. Um Sistema de Registro Eletrônico de Saúde (S-RES)[162] pode ser definido como um "sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde". Sendo a informação identificada tida por aquela que permite individualizar um paciente. O que, por sua vez, abrange não apenas o seu nome, mas também números de identificação como RG e CPF ou outros dados de individualização da pessoa.

Esse sistema é atual, apesar do que se dispôs outrora quanto a revogação de convenio entre que o CFM e a Sociedade Brasileira de Informática em Saúde (SBIS) pela Resolução nº 2.218/2018 do próprio CFM, o Processo de Certificação de S-RES foi criação recente.

O mecanismo sob análise trouxe uma lista de requisitos criados com base em diversos padrões, normas e boas práticas de qualidade de S-RES, os quais foram amplamente discutidos e consensuados por especialistas na área de informática em saúde. Ressaltando, também, que os requisitos constantes neste Processo de Certificação foram submetidos à consulta pública, havendo uma colaboração para seu aperfeiçoamento.

Cabe encerrar a presente disposição com algumas considerações quanto a outros deveres inerentes a essa dinâmica de proteção de dados. Passa-se, pois, a uma análise suscinta quanto ao consentimento informado do paciente.

2.3.3 Consentimento informado como fator relevante no cenário de vulnerabilidade acrescida ao sistema digital

O dever de informar por parte do fornecedor de produtos e serviços que, mesmo de modo potencial, sejam nocivos ou perigosos à saúde faz parte do arcabouço protetivo brasileiro e visa salvaguardar não só a proteção do próprio consumidor, mas também da relação de confiança que este possui com aquele. Este preceito encontra-se expressamente disposto nos artigos 6º, III, e 9º do Código de Defesa do Consumidor, os quais ressaltam, ainda, que tal informação precisa ser ostensiva, adequada e clara.

---

[162]SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE (SBIS). **O que é Certificação de S-RES SBIS.** 2023. Disponível em: http://sbis.org.br/certificacao-sbis/. Acesso em: 8 jan. 2024.

Trazendo a presente normativa para a relação médico-hospitalar, percebe-se que tal encontra-se diretamente vinculada com o imprescindível consentimento informado que provem da exigência de dar a oportunidade à pessoa de eleger, na medida da sua capacidade, se irá se submeter ou não ao serviço oferecido, este tido em sua percepção mais ampla.

Nesse sentido, e em sede de disposições preliminares, o professor doutor Éfren Lima, em seu artigo "Daños Por Violación Delos Deberes Informativos Del Consentimento Informado"[163], defende que toda obrigação resulta em um comportamento do devedor destinado a satisfazer o interesse do credor. Para a relação médica, a concretização desse interesse perpassa, para o autor, não só pela necessidade de informar o paciente, como também pela obrigação de abster-se de prosseguir em determinado ato que esteja sem ou contra a manifestação de vontade do paciente.

Assim, fora posto em ênfase que essa informação prestada ao paciente era fundamental para que este consiga tomar uma decisão que não seja precipitada, bem como incólume de equívocos, de modo a salvaguardar a liberdade e a integridade da pessoa. Há, portanto, uma constante busca pela segurança das protetivas em comento, que, para Bioni, é consequência lógica das incertezas criadas pela ausência de uma engenharia contratual completa[164].

Nessa esteira, acrescenta Gustavo Tepedino e Chiara Spadaccini, por meio do artigo "O Consentimento na Circulação de Dados Pessoais"[165], que a base legal do consentimento para o tratamento de dados do titular representa um instrumento de autodeterminação e livre construção da esfera privada. Este possibilita a compreensão quanto às escolhas e configurações em ferramentas tecnológicas, o que pode ter reflexos diretos quanto às adequadas expectativas de segurança no armazenamento de dados que cabem ser criadas.

---

[163] LIMA, Eduardo Picanço Pinto de Souza. Daños por violación de los deberes informativos del consentimiento informado. **Revista IBERC**, v. 02, n. 02, p. 01-19, mai./ago. 2019. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/52/42. Acesso em: 15 out. 2023.

[164] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 226.

[165] TEPEDINO, Gustavo; SPADACCINI, Chiara. O Consentimento na Circulação de Dados Pessoais. **Revista Brasileira de Direito Civil – RBDCivil**. Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. Disponível em: https://www.rbdcivil.com.br/revista/edicao-25/o-consentimento-na-circulacao-de-dados-pessoais. Acesso em: 05 jun. 2024.

Ademais, Tepedino e Spadaccini versam sobre a chamada razoável expectativa de privacidade, a ser construída caso a caso, como meio de proteção da pessoa humana e incentivo à lealdade recíproca e mútua confiança nas relações. Acrescentando que:

> Todavia, a adoção do critério da legítima expectativa somente se justifica se a ponderação conseguir se desprender da lógica proprietária que, tradicionalmente, acaba por associar a liberdade existencial à prerrogativa de se murar contra agressões alheias ou interferências externas.

Outrossim, os autores asseveram que quando se gerencia o tratamento de informações pessoais, não se resguarda apenas o indivíduo cujos dados estão relacionados, que no vertente caso é o paciente, mas também o grupo social do qual ele faz parte.

Ora, trata-se de uma relação que, a princípio, envolve apenas as partes, mas que possui como base uma atuação com ingerência nos interesses coletivos e que afeta, por certo, as futuras gerações. Assim, evidencia-se que o maior cuidado com o consentimento do titular mostra-se de grande relevância no cenário tecnológico atual.

Isso porque, conforme arguem, atualmente se verifica, de modo muito mais evidente, a coleta em massa de dados pessoais, a mercantilização desses bens por parte de uma série de sujeitos e a ocorrência de situações cuja transparência encontra-se mitigada no que tange ao tratamento de dados.[166]

Partindo desse pressuposto, bem como tomando por base a extrema importância da efetivação do presente consentimento e visando uma abordagem mais clara do exposto, Lima[167] acrescenta a distinção[168] entre os deveres informativos objetivos típicos e atípicos. Os primeiros estão relacionados com a intervenção a ser adotada, ou seja, o protocolo escolhido tanto no aspecto clínico quanto nos âmbitos correlacionados àquela prestação, como o caso das práticas adotadas para tratamento de dados.

Já os deveres atípicos, por sua vez, não são habituais. Requerendo, os primeiros, uma carga informativa mais elevada, ante a sua recorrência e ampla possibilidade de

---

[166] TEPEDINO, Gustavo; SPADACCINI, Chiara. O Consentimento na Circulação de Dados Pessoais. **Revista Brasileira de Direito Civil – RBDCivil**. Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. Disponível em: https://www.rbdcivil.com.br/revista/edicao-25/o-consentimento-na-circulacao-de-dados-pessoais. Acesso em: 05 jun. 2024.

[167] LIMA, Eduardo Picanço Pinto de Souza. Daños por violación de los deberes informativos del consentimiento informado. **Revista IBERC**, v. 02, n. 02, p. 0119, mai./ago. 2019. Disponível em:https://revistaiberc.responsabilidadecivil.org/iberc/article/view/52/42. Acesso em: 15 out. 2023.

[168] *Ibid.*

concretização, ao passo que os últimos podem comportar uma passagem da informação proporcionalmente menor.

Dispondo, mais, que quanto menor for a potencialidade do dano, menos informação seria requerida em termos de repasse. Acrescentando, também, que haveriam os deveres informativos mínimos nos casos de menor potencialidade danosa e deveres informativos adicionais nas hipóteses de maior potencialidade danosa. Ressaltando, também, a existência de um julgado do Supremo Tribunal de Justiça[169] (STJ), segundo o qual defende-se o critério da proporcionalidade direta entre a informação, os ricos inerentes e potenciais de danos, ou seja, quanto maior o risco, maior deveria ser a informação.

Nesse diapasão, trazendo as presentes disposições para a situação ora versada, fica evidente a necessidade que a instituição hospitalar, a qual coletará os dados sensíveis do paciente, possui de informá-lo quanto aos ricos inerentes ao uso das tecnologias de armazenamento de dados para a prestação de serviço oferecido.

Ora, mesmo com a utilização dos mais modernos sistemas, sabe-se que indivíduos altamente qualificados que estão completamente a parte da presente relação podem ter, de modo indevido, acesso ao conteúdo por lá disponibilizado. Portanto, deve ser avisado ao paciente de modo claro, inequívoco e expresso. De modo que tal possa avaliar se está ou não disposto a enfrenta-lo.

Possibilitando, inclusive, a construção da legitima expectativa de segurança, a qual é extremamente relevante para a própria compreensão do conceito de defeito do serviço, que fora fornecida pelo art. 14, §1º, do CDC. Inclusive, cujo caput reitera a necessidade de uma informação suficiente e adequada sobre a fruição e riscos do serviço prestado.

Desse modo, nos casos em que esta não for repassada ou que, mesmo existindo, a informação não seja devidamente esclarecedora, está-se diante de um consentimento viciado. Este que acarreta uma prestação de cuidados com a saúde que carece de validade nos casos dos protocolos clínicos e presume-se segura, nos casos gestão de dados. Hipótese esta que enseja, portanto, a responsabilidade da instituição, a qual será analisada conforme o caso concreto.

---

[169] BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 971.845/DF**. Rel. Nancy Andrighi. Diário da Justiça Eletrônico, nº 269, de 01/12/2008. Disponível em:https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200701573821&dt_publicacao=01/12/2008#:~:text=Trata%2Dse%20de%20recurso%20especial,de%20SERVIER%20DO%20BRASIL%20LTDA. Acesso em: 29 maio 2024.

Assim, a finalidade do consentimento informado é validar a prestação de cuidados de saúde e gestão dos dados, inclusive, funcionando como condicionante da prestação seguinte, devendo ser precedida da soberana decisão do paciente norteada, por sua vez, pelo necessário esclarecimento obtido por meio das informações clínicas [170] e setoriais.

Cabendo ressaltar que o dano gerado pela violação do consentimento em comento não depende da verificação do cumprimento ou incumprimento da prestação dos cuidados técnicos e das opções tecnológicas.

O que, conforme Cordão, nos permite apreciar a autonomia do consentimento livre e esclarecido em relação a prestação propriamente dos serviços em questão. Este que é, nesse sentido e contexto, exigência constitucional estrita para o exercício da autodeterminação informacional, integrando o próprio conteúdo essencial do direito fundamental.

No âmbito da LGPD[171], o consentimento foi mencionado em tópico dos artigos 7º ao 10º da normativa. Delimitações com o dever do seu fornecimento ocorrer por escrito ou por outro meio que demonstre a manifestação de vontade do titular, foram estabelecidos pela normativa.

Ademais, a LGPD acrescenta disposições quanto ao ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta lei ser demonstrado pelo controlador e, expressamente, veda o tratamento de dados pessoais mediante vício de consentimento. Ratificando, mais, orientações quanto à observância de finalidades determinadas adequadamente externadas e a necessidade da adoção de autorizações específicas.

Para além do panorama geral mencionado, a legislação supra traduz uma relevante autonomia do titular dos dados, por meio de disposições que asseguram a possibilidade de o consentimento ser revogado a qualquer momento mediante manifestação expressa daquele. Respaldando, mais, que este procedimento deve ser gratuito e facilitado.

---

[170] LIMA, Eduardo Picanço Pinto de Souza. Daños por violación de los deberes informativos del consentimiento informado. **Revista IBERC**, v. 02, n. 02, p. 0119, mai./ago. 2019. Disponível em:https://revistaiberc.responsabilidadecivil.org/iberc/article/view/52/42. Acesso em: 15 out. 2023.

[171] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

Acrescentando, também, uma prerrogativa para os controladores de dados de terem ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado, isto enquanto não houver requerimento de eliminação[172].

[172] *Ibid.*

3 RESPONSABILIDADE CIVIL NOS CASOS DE ATAQUE HACKER

3.1 OS PRESSUPOSTOS DA RESPONSABILIDADE CIVIL HOSPITALAR

3.1.1 Dano como requisito para responsabilidade do hospital

Inicialmente, urge tecer algumas considerações quanto a existência de requisitos para a aplicação da responsabilidade civil. Tais pressupostos devem ser cuidadosamente observados. Respeitando, conforme o caso, as excludentes inerentes à teoria do processo reparatório. Do contrário, a médio prazo, a inobservância de tais requisitos, necessários ao embasamento do dever de indenizar, ocasionaria o colapso do sistema[173]. Passa-se, pois, a analisa-los.

Em linhas introdutórias, tem-se o art. 186 do Código Civil, que consagra a regra de que todo aquele que causar dano a outrem deve ser obrigado a repará-lo. Quer seja por ação ou omissão voluntária, negligência ou imprudência. Assim, ao violar determinado direito e, por conseguinte, causar dano a outrem, cometerá ato ilícito. Acrescentando, mais, que a vertente disposição será aplicável ainda que o dano seja exclusivamente moral.

Dessa estrutura normativa, alguns elementos inerentes à presente propositura se sobressaem. Dentre os quais, tem-se uma conduta, camuflada pela ideia de ação ou omissão, um elemento volitivo, associado à ideia de culpa ou dolo do agente, uma relação de causalidade, verificada entre a conduta e a consequência, e um dano experimentado pela vítima.

Ademais, ressalta-se que a responsabilidade pode derivar de condutas relativas a “ato próprio” do responsável pela reparação, de “ato de terceiro que esteja sob a guarda do agente”[174] reparador ou a ele vinculado, e ainda de danos causados por coisas e animais que lhe pertençam. Podendo, também, fundamentar-se em uma omissão à deveres juridicamente exigíveis, a exemplo da inobservância do dever de segurança para com os

---

[173] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[174] GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 18ª edição. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

dados dos clientes atendidos por determinada empresa, como é o caso da vertente pesquisa.

Outrossim, fala-se em elemento volitivo, o qual é dividido pela doutrina em dolo e culpa. Sendo o dolo associado ao desejo “próprio” ou à “vontade” intencional de cometer uma violação de direito[175], e a culpa marcada por uma falta de diligência, associada à negligencia, imprudência e imperícia. Os quais devem ser comprovados para a obtenção da reparação, especialmente considerando uma responsabilização subjetiva.

Contudo, esse elemento acaba sendo afastado em alguns casos, dando espaço para a objetificação da reparação. Em que, a conjuntura do caso concreto fundamenta, conforme exposições anteriores, a prescindibilidade da aplicação do elemento culpa, este tido em seu sentido mais amplo.

Um outro pressuposto de relevante menção é o nexo de causalidade, o qual ganha contornos ainda mais evidentes nas hipóteses legais de aplicação da responsabilidade objetiva outrora mencionada. A relação de causalidade sob análise, a qual terá aprofundamento próprio em tópico específico, apresenta-se como a relação de causa e efeito entre a conduta do agente e o dano devidamente verificado. Inclusive, como mecanismo de manutenção funcional do sistema que fundamenta o processo de responsabilização.

Assim, esse nexo se torna imprescindível para a própria existência do dever de indenizar. A existência de um dano desconectado da conduta não deflagra o processo de indenizatório. Sendo, pois, de fundamental observância.

Quanto ao dano, este se divide em patrimonial e extrapatrimonial, ou seja, respectivamente com e sem repercussão na órbita financeira do ofendido. Sobre esse elemento, cabe mencionar que a doutrina majoritária se finca no pressuposto de que sem a prova do dano, ninguém poderia ser civilmente responsabilizado. Comprovação esta que pode estar atrelada à dimensão do dano, como nos casos de prejuízos materiais, ou na ocorrência de lesão a bem ou interesse juridicamente tutelado.

Porém, apesar da inexistência de dano ser óbice à pretensão de uma reparação, alguns doutrinadores fundamentam a possibilidade de uma reparação pautada na barreira ao ilícito lucrativo, que transcende a ideia do dano. De posse dessas noções introdutórias,

---

[175] GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 18ª edição. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

cabe a realização de uma análise quanto ao elemento do dano sob as lentes das discussões até então realizadas.

Antes de uma discussão mais precisa sobre o tema em questão, cabe evidenciar a distinção entre as esferas de responsabilidade, voltando-se para uma adequada categorização do mecanismo trazido pela esfera cível. Considerando, em especial, o que concerne à distinção entre o aspecto penal e o cível. Esta categorização mostra-se como especialmente relevante frente ao surgimento de diversos debates jurídicos quanto ao âmbito de atuação da responsabilidade cível.

O ponto de partida para esta distinção está na origem do conceito de responsabilidade, o qual, para Bioni[176], era tido de modo unitário e era traduzido pela noção de equilíbrio, em relação de causa e efeito, guiada pela ideia de ofensa à norma, a qual ensejaria o reconhecimento e a aplicação de determinada sanção.

Atualmente, vislumbra-se uma especialização das relações jurídicas e de sua respectiva disciplina. O que antes tinha uma acepção subdividiu-se em algumas espécies, dentre as quais a responsabilidade: civil, penal, administrativa e a política. Para a vertente pesquisa, urge a apresentação apenas de uma distinção, em linhas superficiais, entre a responsabilidade cível e a penal, apenas como um norte de aprofundamento da responsabilidade que o estudo se propõe a pesquisar.

Trazendo algumas lições de Carlos Gonçalves[177], tem-se uma responsabilidade civil concentrada nos danos causados à vítima do evento indesejado, de modo a regular questões inerentes à indenização ou a recomposição do patrimônio jurídico lesado, suscetíveis ou não de avaliação econômica. Por outro lado, tem-se uma responsabilidade penal voltada para a manutenção da paz social, à segurança pública, individual e coletiva. Evitando, pois, os chamados crimes expressos na norma em decorrência do seu caráter gravoso a interesses socialmente relevantes, os bens jurídicos.

Para a vertente análise cabe o enfoque em determinados aspectos específicos dessa distinção. O primeiro inerente ao elemento culpabilidade, o qual é amplamente presente no direito penal, ante sua função eminentemente sancionatória. Já para a responsabilidade

---

[176] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 59.

[177] GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 18ª edição. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

civil, os elementos dolo ou culpa podem ser afastados por norma expressa nesse sentido, ocasionando a mencionada responsabilidade objetiva outrora tratada.

Ressaltando, mais, o aspecto da consequência jurídica. No direito penal, a pena não ultrapassa a figura do réu, conforme preceitua o 5º, XLV da CF, o qual elucida o chamado princípio da Intranscendência. Ao passo que a responsabilidade civil incide sobre o patrimônio daquele a quem se imputa responsabilidade. O que pode não ser exatamente quem causou o dano, já que existem casos em que a lei lhe imputa diretamente a responsabilidade a determinado agente em decorrência da sua atividade ou condição jurídica.

Ademais, no sistema penal fala-se em responsabilidade pessoal, não propriamente patrimonial. De modo que, as penas atuam como consequência do cometimento do ilícito, agindo, pois, com a finalidade de castigo, proporcionando um desestímulo à repetição da conduta.

No direito penal, como regra, as penas são privativas de liberdade ou mesmo restritivas de direitos daquele considerado responsável pelo ilícito. Estas culminadas, de modo excepcional, à condenação ao pagamento de multa, que, como bem recorda Gonçalves[178], embora tenha caráter patrimonial, tem por finalidade castigar o criminoso.

Diferente do que ocorre na responsabilidade civil, cujo aspecto patrimonial acaba sendo relevante, posto que se finca em uma busca pela recomposição patrimonial da vítima ou na indenização referente a abalos não economicamente auferíveis. Partindo das distinções supramencionadas tem-se que a figura do dano se evidencia como pressuposto da aplicação do instituto da responsabilidade civil.

Inclusive, conforme preceitua o art. 944 do CC, a indenização é medida pela extensão do dano, podendo, conforme disposição expressa em seu parágrafo único, ser reduzida, equitativamente, nos casos de excessiva desproporção entre a gravidade da culpa e o dano gerado no caso concreto.

Nesse ponto, cabe mencionar que que alguns autores relevantes no cenário nacional fundamentam a multifuncionalidade da responsabilidade civil[179]. Defendendo, pois, que

---

[178] GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 18ª edição. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

[179] ROSENVALD, Nelson. **A Responsabilidade Civil pelo Ilícito Lucrativo**. 2 ed. Salvador: Juspodvim, 2021. p. 224.

esta deve ser dinâmica e dotada de flexibilidade suficiente para reestabelecer o equilíbrio desfeito à custa do dano.

Assim, fundamentam quanto a possibilidade de uma reparação que ultrapasse a esfera compensatória e passe a abarcar a restituição de lucros ilícitos. Buscam, pois, não apenas a reposição da vítima ao "estágio pré-dano", mas também a restituição do ofensor "ao estado pré-ilícito".

Contudo, apesar da relevância da doutrina supramencionada, a vertente pesquisa não se aprofundará nos nortes doutrinários por ela abraçados. Especialmente considerando a conexão do seu cerne com teses norteadas por uma função punitiva da responsabilidade que muito se vincula a uma busca pela inibição da conduta do agente causador do dano. Não sendo, pois, o presente foco.

Nesse sentido, passa-se a uma análise quanto a um outro pressuposto de extrema relevância para a dinâmica reparatória, o denominado nexo de causalidade e as suas teses de aplicação.

3.1.2 Nexo de causalidade do incidente de segurança envolvendo dados sensíveis

Considerando as discussões outrora delineadas, cabe tecer algumas projeções quanto ao nexo causal, este tido como o vínculo entre as consequências danosas e a conduta do indivíduo apontado como responsável pela reparação, ou seja, "o nexo etiológico material que liga um fenômeno a outro"[180].

Requisito este que ganha contornos relevantes em um cenário de aplicação da responsabilidade civil objetiva. Posto que, retira-se o foco da existência de dolo ou culpa, concentrando a deflagração do dever de indenizar na existência de um dano vinculado a uma conduta ou omissão ilícita de um agente.

Nesse ponto, Tepedino[181] traz à baila a tese da dupla função do nexo causal, segundo o qual o vínculo em comento atuaria como fator elementar para a verificar a extensão do dano indenizável, bem como auxiliaria na própria determinação de a quem se

---

[180] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[181] *Ibid.*

deve atribuir o resultado danoso. Acrescentando, mais, que houve uma modificação quanto ao entendimento que norteia a medida da reparação[182].

De modo que, anteriormente, a visão predominante pautava-se na culpabilidade para averiguar os contornos indenizatórios. Entretanto, o contexto atual vincula-se à causalidade para estipular o quantum adequado devido à casuística apresentada[183]. Assim, sobram evidencias quanto a relevância dessa estrutura na análise da responsabilidade civil.

De posse da relevância da mencionada estrutura, cabe um aprofundamento quanto às teorias que se propõem a delimitar a forma de incidência do nexo de causalidade. Ressaltando, mais, em que medida esta causa torna-se fundamento para a imputação da responsabilidade do agente, conforme cada tese. Já que a contribuição do fato para o dano pode assumir diferentes graduações. Assim, a definição quanto a qual teoria explicativa do nexo causal deve ser admitida "poderá determinar conclusões diversas sobre a aptidão do fato como critério de imputação da responsabilidade do agente"[184].

Inicialmente, traz-se à baila a teoria da equivalência das condições, estruturada pelo penalista alemão Von Buri, em 1860[185]. Segundo a qual todas as circunstâncias que tenham concorrido para produção do dano são consideradas como possíveis causas. Assim, qualquer evento que, por si só, for capaz de gerar o dano seria tido como causa suficiente para ensejar a reparação, ou seja, o evento atuaria como condição *sine qua non* para que o dano se verificasse.

Essa tese possui uma vocação expansiva da relação de causalidade, considerando a sucessão cronológica dos acontecimentos. Dessa forma, qualquer um daqueles que promovem um dos eventos da cadeia causal poderá ser responsabilizado pelo dano sofrido pela vítima[186].

---

[182] PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de direito privado**. 3. ed. Rio de Janeiro: Editor Borsoi, 1971. v. 22, p. 202.
[183] *Ibid.,* p. 202.
[184] MIRAGEM, Bruno. **Responsabilidade Civil.** Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 fev. 2024.
[185] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.
[186] MIRAGEM, *op. cit.,* p. 48.

Entretanto, a teoria em comento pode, segundo Gonçalves[187], conduzir a resultados absurdos dentro do direito. Especialmente quando se vislumbram toda sorte de antecedentes para justificação do resultado danoso, os quais são, por vezes, irrelevantes.

Assim, a tese desconsidera a maior ou menor proximidade das condições que originaram o resultado, sendo todas reputadas, para fins de responsabilidade, equivalentes. Gerando, pois, uma teia ilimitada de causas e agentes por ela responsáveis[188]. Oferecendo, também, excessiva margem de discricionariedade ao intérprete, posto que não delimita critérios adequados à redução do exame objetivo das causas, as confundindo com as várias condições atreladas ao evento danoso.

A segunda teoria, conhecida como da causalidade próxima, proposta por Francis Bacon, delimitou que a causa cronologicamente mais próxima ao evento danoso deveria servir para a imputação da responsabilidade, dispensando a investigação das causas mais remotas. Esta tese adota uma percepção de que a última condição, tomando como referência uma cadeia causal concreta, é a que resulta na produção do dano, promovendo a unidade lógica e finalística ao conjunto de causas do evento[189].

Contudo, não faltam críticas para a aplicação da vertente tese. As quais ficam-se, especialmente, na dificuldade de identificação da causa mais próxima ao dano e no fato de que esta nem sempre será fator determinante para a estruturação da conjuntura danos. Gerando, pois, uma imprecisão nos seus comandos.

Outrossim, uma outra tese que ganha contornos no cenário doutrinário é a teoria da causa eficiente. Segundo Herrera[190], tal tese parte do pressuposto que as diversas condições do dano não são idênticas, mas definem diferentes contribuições para a realização do evento danoso.

Portanto, caberia à vertente teoria, por meio de critérios quantitativos e qualitativos, a identificação quanto a qual causa fora determinante para o evento danoso, ou seja, qual a que contribuiu em maior medida para a produção do resultado.

---

[187] GONÇALVES, Carlos Roberto. **Responsabilidade civil**. São Paulo: Editora Saraiva, 2024. E-book. ISBN 9786553629479. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553629479/. Acesso em: 23 abr. 2024.

[188] ALVIM, Agostinho Neves de Arruda. **Da inexecução das obrigações e suas consequências**. 4. ed. São Paulo: Saraiva, 1972, p. 345.

[189] COSTA JÚNIOR, Paulo José. **Nexo causal**. 3. ed. São Paulo: Siciliano Jurídico, 2004, p. 104.

[190] HERRERA, Edgardo López. **Teoría general de la responsabilidad civil**, cit., p. 202; HONORÉ, A. M. Causation and remoteness of damage, cit., p. 38-39.

Desse modo, evidencia-se que a avaliação quanto à eficiência da causa não se dá em abstrato. Havendo, em verdade, um elemento comparativo responsável pela distinção entre a causa que produz o resultado e as outras condições que não foram suficientes para produzi-lo, mas reduziram ou aumentaram as barreiras para a sua produção. Esta tese também não foi isenta de críticas. Em especial, ante a ausência de critérios definidos para se estabelecer uma ordem de importância entre os vários eventos do processo causal[191].

Para além das teorias outrora analisadas, cabe tratar sobre a causalidade necessária, explicitada pela teoria do dano direto e imediato. Também conhecida como interrupção do nexo causal por alguns autores[192], a qual representa um amálgama entre a teoria da equivalência e a da causalidade adequada[193]. Tida, pois, como um meio-termo entre tais teses.

A teoria em questão fora consagrada pelo codificador pátrio no art. 403 do Código Civil, segundo a qual, apenas se consideram causas as vinculadas ao dano direta e imediatamente, isso considerando até mesmo um cenário de inexecução contratual resultante de dolo do devedor. Esse dispositivo, por mais que esteja vinculado expressamente às consequências do inadimplemento contratual, tem a sua interpretação aplicada, também, às dinâmicas inerentes ao processo reparatório.

A causalidade necessária, em suma, busca identificar a conduta ou omissão a qual atue de tal forma que, caso não existisse, não poderia materializar o dano. Ou seja, se a cadeia causal de acontecimentos tivesse se rompido pela interrupção do nexo causal, o dano não teria se efetivado.

Assim, independem do lapso temporal entre sua ocorrência e a materialização do dano. De modo que, tal dinâmica de vinculação passa a ser condição para a reparação. Assim, existindo alguma circunstância posterior que efetivamente conduza, por si, ao resultado danoso, haveria a ocorrência de uma interrupção da conexão entre a primeira causa e o dano.

---

191 MIRAGEM, Bruno. **Responsabilidade Civil.** Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 fev. 2024. p. 136

192 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

193 GONÇALVES, Carlos Roberto. **Responsabilidade civil.** São Paulo: Editora Saraiva, 2024. E-book. ISBN 9786553629479. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553629479/. Acesso em: 23 abr. 2024.

Nesse sentido, Tepedino[194] acrescenta que não se trata da distância temporal entre a consequência danosa e a conduta do agente que rompe o nexo causal, “mas, sim, a interferência de outra cadeia causal independente”.

Portanto, as consequências danosas, mesmo que estejam distantes, temporalmente, da conduta do agente são passíveis de ressarcimento. Isso desde que atuem como consequência direta e imediata de um ato ilícito ou de uma atividade tida como objetivamente perigosa. Estando, pois, ligados à conduta do agente por uma cadeia causal que não tenha sofrido qualquer interrupção.

Nota-se que, ao adotar a teoria em questão, não caberia submeter o autor do dano a qualquer consequência de sua conduta, senão apenas àquelas que sejam diretamente ligadas a ele[195]. Logo, a vertente tese estabelece muito mais que um critério para imputação da responsabilidade, mas também atua na formação de limites para a extensão desta reparação. Impossibilitando, pois, a aplicação de uma responsabilização ilimitada[196].

Contudo, essa teoria não é isenta de críticas. Dentre as quais, cabe mencionar que a adoção de tal tese poderia culminar na exclusão dos chamados danos indiretos ou reflexos. Isso, porque estes ao não possuírem uma imediata vinculação com o fato atribuível ao agente, acabam distanciando-se da causa fundamentadora da reparação[197].

Ademais, a doutrina contrária à vertente tese argumenta, também, que a exigência de que a causa tida como ocasionadora do dano seja necessária e suficiente acaba por ignorar a possibilidade de o caso concreto envolver uma multiplicidade de causas, todas concorrendo para a produção do dano.

Entretanto, Miragem[198] dispõe quanto a possíveis respostas para as contrariedades suscitadas. Dentre as quais, lista-se a possibilidade de a sucessão causal normal contemplar o dano reflexo como dano indenizável resultante da consequência danosa tida como principal. Bem como, pontua que como consequência da adoção de uma condição

---

194 TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

195 CRUZ, Gisela Sampaio da. **O problema do nexo causal na responsabilidade civil.** Rio de Janeiro: Renovar, 2005.

196 MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 fev. 2024.

197 *Ibid.,* p. 162.

198 *Ibid.,* p. 163.

tida como necessária para a realização do dano, tem-se que a exclusão da responsabilidade civil só será possibilitada com a demonstração do rompimento do nexo causal. Sendo tal interpretação de extrema relevância para a compreensão do art. 403 do Código Civil.

Entretanto, a despeito das teorias mencionadas, os tribunais costumam invocar a causalidade adequada para fundamentar o processo decisório. De modo a demonstrar que o dever de reparar advém da necessária conexão existente entre o dano e a atividade.

Nesse sentido, tem-se o entendimento do STJ[199] nos embargos de declaração no agravo em recurso especial nº 2490156 -SP de relatoria da Ministra Maria Isabel Gallotti. O qual, retomando as lições de Sergio Cavalieri Filho, ressaltou a aplicação da teoria da causalidade adequada pelo nosso ordenamento jurídico. Acrescentando, mais, que nem todas as condições que concorrem para o resultado são equivalentes, mas somente aquela que for a mais adequada a produzir concretamente o resultado.

Para uma adequada compreensão dessa adoção, cabe elucidar quanto a alguns aspectos relevantes da teoria denominada de causalidade adequada[200], a qual sustenta que apenas atua como originadora do dano a condição que por si só é apta a produzi-lo. Atuando, pois, a causa como elemento adequado para a produção do efeito, desconsiderando circunstancias acidentais, inaptas para a produção das consequências danosas.

Um exemplo doutrinário comum a essa tese é o da ocorrência de um incêndio em determinado condomínio residencial ou comercial causado por um curto-circuito elétrico em uma das unidades. Nesse caso, demonstrado que o apartamento não possuía a estrutura elétrica requerida pelas normas de segurança, o proprietário deste imóvel se responsabilizaria pelos dados decorrentes do evento em questão.

Ao passo que, tendo o curto-circuito sido apenas uma das causas do incêndio, mas que o fator determinante para a ocorrência do dano fora a falta de equipamentos de segurança, pode-se fundamentar, por esta teoria, que essa condição é a causa adequada para a efetivação dos danos causados pelo evento descrito.

---

[199] BRASIL. Superior Tribunal de Justiça. **EDcl no AREsp 2490156**. Rel. Min. Maria Isabel Gallotti. Brasília, DF, 07 mai. 2024.

[200] GONÇALVES, Carlos Roberto. **Responsabilidade civil**. São Paulo: Editora Saraiva, 2024. E-book. ISBN 9786553629479. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553629479/. Acesso em: 23 abr. 2024.

A percepção quanto a aptidão ou não da causa se apoia em uma análise que requer abstração[201]. Ou seja, abstratamente o fato que ocasionou o dano era capaz de lhe dar causa, configurando-se nos mais variados casos dessa natureza. Sendo, pois, causa adequada ao efeito materializado. Contudo, sendo uma consequência de uma mera circunstância acidental, não caberia a arguição de adequação causal[202].

Em suma, a teoria sob análise define um método que resulte na identificação, dentre os antecedentes do dano, e no conseguinte afastamento daqueles menos relevantes para a sua ocorrência. Resultando, apenas, na conduta necessariamente concretizadora do dano. O que, segundo Miragem[203], resulta na aproximação da teoria da causa adequada e da tese da interrupção do nexo causal.

Esse fenômeno decorre, em especial, na jurisprudência brasileira. Isso, porque os julgados optam pela adoção nominal da teoria da causalidade adequada, porém, ao analisar os fundamentos do *decisum*, parecem induzir a aplicação do critério da causalidade necessária.

Diante das teses e fundamentações expostas, pode-se perceber que a doutrina qualificada opta, majoritariamente, pela compreensão que o responsável pelo evento danoso não responde de maneira ilimitada pelas consequências inerentes a sua conduta ou inação. Existindo, assim, hipóteses excepcionais em que o dano não será acompanhado da correlata reparação, especialmente se estivermos diante de um cenário de rompimento do nexo causal.

Por meio da vertente conclusão, cabe elucidar alguns pontos concernentes ao rompimento da conexão entre o dano e a conduta, ou inação, do responsável pela reparação, os quais ganham contornos significativos para a presente pesquisa. Especialmente considerando um cenário de aplicação da responsabilidade objetiva em que, conforme exaustivamente exposto, o nexo causal ganha contornos ainda mais evidentes, pela irrelevância do elemento dolo ou culpa.

---

[201] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 23 fev. 2024.
[202] ALVIM, Agostinho Neves de Arruda. **Da inexecução das obrigações e suas consequências**. 4. ed. São Paulo: Saraiva, 1972, p. 345.
[203] MIRAGEM, *op. cit.,* p. 144.

3.1.3 Hipóteses de isenção da responsabilidade do hospital

Em linhas gerais, para o direito privado, o rompimento do nexo de causalidade entre o dano e o responsável pela reparação pode ser ocasionado por um fato exclusivo da vítima ou de terceiro, ou nos casos de fortuito e força maior. Ou seja, admite-se a possibilidade de uma causa autônoma interferir na cadeia causal a modificando de tal forma que imporá a exclusão da responsabilidade de quem, inicialmente, competia o dever de indenizar[204].

Assim, mesmo havendo a materialização inequívoca de uma consequência danosa, ao agente não competirá mais a obrigação de reparar o dano, ante ao rompimento da cadeia causal original.

Nesse ponto, Tepedino[205] elucida, de modo didático, alguns pontos relevantes quanto a cada uma das hipóteses supramencionadas. Dispondo, inicialmente, quanto ao fato exclusivo da vítima. Segundo o qual o indivíduo que suporta o dano concorreu, exclusivamente, para a consequência negativa em questão. Afastando, assim, a obrigação reparatória a quem era imputado o ônus de arcar com a indenização.

Exemplo evidencia-se com o vazamento de informações pessoais em detrimento do acesso a banco de dados possibilitado pelo repasse, realizado pelo próprio titular, de login e senha de acesso ao sistema. No caso em apreço, a plataforma ou o prestador do serviço não responderiam por eventuais danos dessa ocorrência.

Diferente seria se a passagem desses dados de acesso for parcialmente ocasionada por uma falha estrutural do sistema que atue lincando o titular a um site falso ou qualquer outra falta de diligencia da vítima atuando de modo concorrente com uma conduta do agente.

Nesse caso, em que a conduta do titular dos dados e do agente contribuem para o resultado, tem-se a formação de um nexo causal composto, o qual se associa a ambas as práticas. Respaldando a impossibilidade de isenção do agente, ante a sua parcela de atuação para a promoção do evento danoso, mas caberia uma redução do quantum indenizatório ante a falta de diligencia razoavelmente esperada da vítima,

---

[204] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[205] *Ibid.,* p. 102.

Outrossim, o autor[206] acrescenta quanto à ocorrência do fato de terceiro, o qual apresenta particular relevância para a presente pesquisa. Nessa hipótese de quebra na cadeia causal, o dano decorre direta e imediatamente da conduta de pessoa estranha à relação original que ensejaria a reparação pelo agente sob análise.

Acrescenta, mais, que para efetivamente afastar o dever de indenizar do agente, este não deve ser legalmente responsável pelos danos causados pelos terceiros. Exemplos evidenciam-se com a responsabilidade dos pais pelos filhos menores que estiverem sob sua autoridade, ao empregador, por seus empregados no trabalho ou em razão dele, e em todos os demais casos contidos no art. 932 do Código Civil.

Em consonância com o fato da vítima, a atuação de terceiro só implica na isenção da responsabilidade do agente inicialmente tido como responsável pela reparação, se for exclusiva e autônoma. Caso haja uma concorrência desta conduta com fato atribuível ao agente, o dever de reparar passa a ser requerido. Assim ambos respondem pela composição das perdas e danos. Isto na medida de sua respectiva contribuição.

Outro ponto de relevante observação vincula-se ao fato de que este terceiro deva ser estranho atividade exercida pelo agente, não se inserindo na sua esfera de influência e atuação. Bem como, não deve guardar relação de proximidade com vítima do dano ocasionado.

Nos casos de vazamento de dados médico-hospitalares tal terceiro não pode ser um funcionário dos quadros do hospital ou manter com este qualquer tipo de vínculo, do contrário não caberia qualquer inaplicação do dever reparatório para com o titular dos dados. Configurando, em verdade, um verdadeiro fortuito interno absorvido pelo risco da atividade e passível de manutenção da responsabilização.

Nesse sentido, cabe colacionar a jurisprudência do STJ proferida no julgamento Agravo em Recurso Especial Nº 2547642[207] - RJ. Na qual os acontecimentos se desenrolaram no interior da agência bancária, em horário de expediente, e cujos eventos estejam associados às atividades corriqueiras do banco.

---

[206] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[207] BRASIL. Supremo Tribunal Federal. **AREsp: 2547642**, Relator: Ministra Maria Thereza de Assis Moura, Data de Publicação: 25/04/2024 Disponível em:https://www.jusbrasil.com.br/jurisprudencia/stj/2482880174/inteiro-teor-2482880177

Houve, no caso em questão, uma falha evidente na prestação do serviço, impossibilitando qualquer afastamento da responsabilidade do agente. As nuanças causais envolvem uma movimentação financeira em quantia vultuosa, em completa desconformidade com o histórico do titular da conta.

Ferindo, inclusive, o limite diário de movimentação estipulado, proporcionalmente, pela instituição financeira, bem como demonstrando um irregular conhecimento quanto ao quantum monetário possuído pelo titular da conta. Sem ocasionar, portanto, qualquer dúvida quanto à irregularidade do serviço.

Trata-se, pois, de fortuito interno. No qual, mesmo diante da existência de fato de terceiro, é possível vislumbrar-se “um comportamento esperado e possível do fornecedor de serviços para evitar o dano perpetrado”, conforme pontua a Corte.

Esse entendimento será pontualmente retomado em momento posterior, especialmente para respaldar uma adequada análise dos casos em que a falha na proteção de dados do paciente é ocasionada por uma prestação de segurança informática defeituosa.

Em que se evidencia a não adoção, pela instituição hospitalar, dos requisitos normativos estabelecidos pelo ordenamento jurídico brasileiro, nem a observação dos standards de segurança mínimos. Incrementando os riscos razoavelmente esperados na realização do tratamento de dados de cunho sensível.

Diferente seria no caso do REsp: 2046026 RJ 2022/0216413-5[208] de relatoria da ministra Nancy Andrighi. Segundo o qual o recorrido adquiriu um automóvel inicialmente

[208] CIVIL. RECURSO ESPECIAL. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. CONSUMIDOR. DEFEITO DE FUNDAMENTAÇÃO. NÃO OCORRÊNCIA. EMISSÃO DE BOLETO FRAUDULENTO. RESPONSABILIDADE DA INSTITUIÇÃO FINANCEIRA. AUSÊNCIA. FALHA NA PRESTAÇÃO DOS SERVIÇOS. INEXISTÊNCIA. FATO EXCLUSIVO DE TERCEIRO. 1. (...)2. O propósito recursal consiste em definir se a emissão, por terceiro, de boleto fraudado, configura fato exclusivo de terceiro apto a excluir a responsabilidade civil da instituição financeira.3. (...) . 4. A jurisprudência do STJ compreende que a atividade bancária, por suas características de disponibilidade de recursos financeiros e sua movimentação sucessiva, tem por resultado um maior grau de risco em comparação com outras atividades econômicas. Consequentemente, foi editada a Súmula 479, a qual dispõe que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". 5. Não é prescindível, todavia, a existência de um liame de causalidade entre as atividades desempenhadas pela instituição financeira e o dano vivenciado pelo consumidor, o qual dar-se-á por interrompido caso evidenciada a ocorrência de fato exclusivo da vítima ou de terceiro (art. 14, § 3º, II, do CDC) ou evento de força maior ou caso fortuito externo (art. 393 do CC/02). Qualquer dessas situações tem o condão de excluir a responsabilidade do fornecedor.6. O fato exclusivo de terceiro consiste na atividade desenvolvida por uma pessoa sem vinculação com a vítima ou com o aparente causador do dano, que interfere no processo causal e provoca com exclusividade o dano. No entanto, se o fato de terceiro ocorrer dentro da órbita de atuação do fornecedor, ele se equipara ao fortuito interno, sendo

comprado por meio de financiamento bancário obtido pelo vendedor do veículo junto ao banco recorrente.

No vertente caso, para a quitação do bem, o recorrido assumiu o valor do financiamento que ainda estava pendente de pagamento e realizou a quitação via boleto bancário. Ocorre que, tal documento para quitação não fora emitido pela instituição financeira, mas sim por terceiro estelionatário, bem como fora enviado pelo vendedor do automóvel através de e-mail que não é de titularidade do banco.

Desse modo, a Corte entendeu que não haveria como arguir a existência de falha na prestação dos serviços, posto que a fraude não guardava conexão com a atividade desempenhada pelo banco recorrente. Tendo ocorrido sem qualquer intermédio do agente a quem se buscou imputar a responsabilização.

Restando evidente a caracterização como fato exclusivo de terceiro. Assim, não é dispensável a existência do liame de causalidade entre o dano vivenciado pelo consumidor e as atividades desempenhadas pela instituição financeira. Assim, evidenciada a vertente interrupção na cadeia causal por fato exclusivo de terceiro[209], não caberia a manutenção do dever de indenizar[210].

Note-se, mais, que a análise quanto ao fenômeno capaz de elidir o dever de reparação demanda uma percepção casuística, posto que se encontra em relação de dependência para com a atividade exercida pelo agente.

Nesse ponto, observa-se a dinâmica do risco inerente à atividade propriamente exercida em contrapartida às questões externas do serviço prestado. Passa-se, então, a uma análise quanto dever ou não do fornecedor de serviços de evitar a ocorrência do dano, considerando um cenário de viabilidade para tanto.

Dever este que varia conforme as legitimas expectativas sobre a prestação de serviço requisitada. Em um cenário no qual a tutela dos dados não atua como o objeto principal da prestação, uma fraude praticada por terceiros que não se valham de nenhuma

---

absorvido pelo risco da atividade (...) (STJ - REsp: 2046026 RJ 2022/0216413-5, Relator: NANCY ANDRIGHI, Data de Julgamento: 13/06/2023, T3 - TERCEIRA TURMA, Data de Publicação: DJe 27/06/2023) (grifo meu)

[209] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 29 maio 2024.

[210] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

ferramenta colocada à disposição pelo agente de tratamento de dados pode respaldar o rompimento do nexo causal entre o dano e o fornecedor.

Ademais, para além das hipóteses supramencionadas, cabe acrescentar a quebra da cadeia causal ocasionada pelo caso fortuito ou pela força maior. Cuja ocorrência vincula-se a um acontecimento extraordinário, inevitável e atual[211] responsável por provocar, de modo autônomo, as consequências danosas.

Acrescenta-se que, embora exista uma relevante distinção entre o caso fortuito e a força maior, parte considerável da doutrina entende que estabelecer tal diferenciação não apresentaria, na prática, nenhuma utilidade. Contudo, cabe evidenciar, suscintamente, alguns contornos dessa distinção.

Nesse diapasão, Caio Mario dispõe que embora as consequências destas questões extraordinárias sejam as mesmas[212], o caso fortuito encontra-se associado aos acontecimentos provenientes de forças da natureza, ou o fato das coisas. Ao passo que a força maior ocorre no fenômeno advindo do fato das pessoas, a exemplo das guerras, greves ou revoluções.

Desse modo, essas estruturas podem ser associadas a eventos imprevisíveis e inevitáveis, os quais podem impedir o cumprimento de uma obrigação legal ou ocasionar danos consideráveis. Tais estruturas estão fora do controle das partes e, em determinados casos, podem isentar a responsabilidade pelo não cumprimento contratual.

Inclusive, nesse ponto, cabe acrescentar que a imprevisibilidade do evento não caracteriza de pronto a ocorrência do caso fortuito a isentar o dever de reparação. Já que alguns destes podem ser contornados pela realização de condutas diligentes afastando a inevitabilidade a caracterizar o fortuito.

Ademais, por vezes, até mesmo eventos previsíveis[213] têm o condão de atingir a relação obrigacional de modo a tornarem-se irresistíveis ao devedor, impossibilitando o adimplemento da obrigação. Requerendo, pois, um reajuste contratual a reequilibrar a estrutura acordada.

---

[211] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[212] PEREIRA, Caio Mário da Silva. **Obrigações e contratos – pareceres**, Rio de Janeiro: Forense, 2011, p. 358.

[213] PEREIRA. Caio Mário da Silva**. Instituições de Direito Civil.** Rio de Janeiro: Forense, 2022. v.3. 385.

Tepedino[214] elucida, mais, que para a configuração do fortuito sob análise, precisam ser averiguadas algumas questões. Dentre as quais, se o fato realmente ocasionou o dano arguido, sendo tal evento danoso tido como “necessário, inevitável, irresistível para aquele agente concreto”.

Outrossim, caberia a investigação quanto à inserção do acontecimento nos riscos inerentes, ou expressamente assumidos, à atividade desempenhada. Distinguindo, pois, a ocorrência de situações em que não se afasta o dever de indenizar como nos casos de fortuito interno ou de cláusula contratual de assunção expressa dos riscos do fortuito.

Contudo, a presente pesquisa seguirá as analises subsequentes com um enfoque na hipótese de rompimento do nexo causal em decorrência do fato de terceiro. Especialmente averiguando as disposições normativas pertinentes à Lei Geral de Proteção de Dados e ao Código de Defesa do Consumidor, os quais serão de pertinente direcionamento para as futuras discussões.

3.2 RESPONSABILIDADE DO HOSPITAL E A INTERFERÊNCIA DA CULPA NO INCIDENTE DE SEGURANÇA

Tomando por base os pressupostos outrora apresentados, bem como considerando que a palavra responsabilidade tem origem do latim *respondere*, que sustenta a ideia, para o direito civil, de garantia da restituição ou compensação do bem sacrificado pela vítima, cabe prosseguir no aprofundamento da vertente pesquisa.

Inicialmente, esse sistema inerente ao processo de responsabilização passou por um constante processo de evolução[215], transcendendo a distinção entre dever contratual e extracontratual. Alcançando, pois, uma análise mais profunda do próprio conteúdo do dever cuja violação dá causa à responsabilidade do agente consequente imputação do dever de indenizar.

---

[214] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[215] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 jan. 2024.

Partindo do cenário, cabe uma suscinta disposição quanto ao dever de segurança que conversa amplamente com as questões inerentes à presente pesquisa. Miragem[216] aponta como origem do dever sob análise, no direito brasileiro, as disposições do Código de Defesa do Consumidor.

No direito consumerista, especificamente no art. 8º, está expressamente previsto o dever dos fornecedores de ofertar apenas produtos e serviços que "ofereçam a segurança que legitimamente deles se espera". Assim, trabalha-se com o aspecto dos níveis de risco normais e previsíveis[217], os quais encontram-se intimamente atrelados à prestação de modo abstratamente auferível e amplamente conhecido.

Desse modo, a oferta de riscos anormais será considerada como prestação defeituosa. Ensejando, portanto, a responsabilidade objetiva do fornecedor. Para adequado aprofundamento, será analisado, em momento posterior, alguns aspectos da objetividade e subjetividade da mencionada responsabilização.

Nesse interim, quando for imputado ao agente[218] um dever de prevenir a ocorrência de danos, especialmente nos casos em que a sua conduta der causa a riscos, tidos como anormais, a direitos ou interesses alheios, aquele deve responder pelos que der causa.

Nesse ponto, urge a materialização de uma reflexão que parece ser de extrema relevância para uma abordagem inicial do tema. Um primeiro olhar deve incidir sobre a inexistência de uma segurança plena no ambiente virtual.

Isso deve ser amplamente discutido, requerendo diversas imersões em literaturas na área de pesquisa da computação. Inclusive, porque mesmo os sistemas mais estruturados, em termos de técnicas e *softwares*, podem ser invadidos. Ao que parece fundamentar a existência de um risco padrão e esperado nesse setor.

Com esse pressuposto e considerando as discussões anteriores sobre deveres legais e standards de segurança, pode-se perceber a existência de mecanismos para a manutenção desses riscos em limites aceitáveis, já que o sistema estaria, evidentemente, muito mais protegido.

---

[216] *Ibid.,* p. 77.

[217] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 29 maio 2024.

[218] Para a análise em questão, o agente é o controlador de dados sensíveis dos pacientes. Atuando como prestador do serviço de proteção dos dados na esfera hospitalar.

O descumprimento de quaisquer destes já proporciona o aumento dos riscos de acessos indevidos aos sistemas de armazenamento de dados. O que ensejaria uma possível responsabilização com a ocorrência do dano.

Nesses casos, o fato de ocupar a posição jurídica prevista em lei é suficiente para a imputação do dever de indenizar. Ressalvando-se, porém, a possibilidade da exclusão do dever indenizatório apenas em razão do rompimento do nexo causal, o qual será aprofundado em momento oportuno.

Entretanto, antes da apresentação de contornos mais específicos da vertente questão, cabe um recorte quanto às bagagens teóricas que se mostram imprescindíveis para a discussão da presente temática. Passa-se, pois, à análise de alguns pressupostos dessa dinâmica de responsabilização.

O dever de segurança[219] outrora mencionado, para o direito civil, emerge de várias frentes. Considerando não só o exercício de uma função, a exemplo do risco da atividade perigosa, disposto no art. 927[220] em seu parágrafo único, como também o risco empresarial previsto no art. 931[221]. Abarcando, igualmente, determinada posição jurídica prevista em lei que seja suficiente para imputar responsabilidade, como é o caso das normativas concernentes aos artigos 936 e 937 do Código Civil.

Tendo por base essa disposição, fica evidente que o dever de segurança dos dados sensíveis dos pacientes emerge da atividade empresarial exercida pelo hospital. Dessas considerações surgem, pois, as próximas análises.

3.2.1 Noções introdutórias sobre a responsabilização do hospital por danos causados aos pacientes

Inicialmente, com o intuito de identificar a natureza da responsabilidade civil hospitalar, o doutrinador Miguel Kfouri Neto[222] cita uma relevante sistematização feita pelo

---

[219] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 jan. 2024.

[220] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 29 maio 2024.

[221] *Ibid.*

[222] KFOURI, Maurício Zanoide de Moraes. **Responsabilidade Civil dos Hospitais -** Código Civil e Código de Defesa do Consumidor. São Paulo: Thomson Reuters Revista dos Tribunais, 2022. RB-1.1. Ebook. ISBN

douto Fernández Hierro, na qual distingue a responsabilidade derivada de atos extramédicos, atos paramédicos e atos essencialmente médicos.

A responsabilidade que compete análise para a presente pesquisa é a referente aos atos extramédicos, sob a perspectiva da obrigação de garantir a segurança dos pacientes. Desse pressuposto, cabe mencionar que o aspecto segurança deve incidir sobre várias dimensões de tutela, quer seja física ou psíquica. O que, portanto, engloba o dever de proteção dos dados dos pacientes, em especial os dados sensíveis tratados nessa relação.

Além dos cuidados comuns, o hospital deve adotar todas as medidas para assegurar que dados de natureza tão íntima só sejam acessados quando estritamente necessário e por quem tem autorização pra tanto. Kfouri observa que, em regra, esses serviços extramédicos como o alojamento, alimentação, deslocamento do doente nas dependências do hospital, manutenção e, acrescenta-se, o funcionamento regular dos sistemas digitais de armazenamento de dados e gestão de riscos são desempenhados por pessoal auxiliar, sob as ordens da administração do hospital, requerendo, pois, alguns cuidados.

Essas cautelas são fundamentais para a regular prestação do serviço. Evitando prejuízos morais e materiais aos pacientes. Entretanto, uma vez ocorrido o dano e restando provado o nexo de causalidade, o hospital responderá pelo defeito do serviço, na forma do que preceitua o Código de Defesa do Consumidor. Assim, em um cenário de responsabilização objetiva, uma adequada análise quanto ao nexo causal faz-se primordial para uma adequada deliberação sobre o tema, o que será aprofundado posteriormente[223]

Partindo dos pressupostos acima trazidos, urge delimitar de modo mais preciso sobre a responsabilidade que está sendo analisada, dispondo sobre fatores relevantes para que ocorra a sua incidência. Sempre considerando para a presente pesquisa, a adequada tutela direcionada a proteção dos dados sensíveis dos pacientes.

Uma distinção que se faz necessária para o aprofundamento da matéria é entre a responsabilidade subjetiva e objetiva. A primeira vinculada à ideia de culpa. Posto que, para tal, a adequada prova da culpa do agente passa a ser pressuposto do dano indenizável[224], de modo que a responsabilidade do causador do dano se configura mediante a conduta

---

9786559910489. Disponível em:https://nextproview.thomsonreuters.com/launchapp/title/rt/monografias/105155050/v5/page/RB-1.1%20. Acesso em: 22 nov. 2023.

[223] GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 18 ed. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

com dolo ou culpa do agente. Não havendo o que dispor sobre a responsabilidade civil, nos casos de não configuração de um ou outro elemento.

Miragem[225] aponta que antes a noção de culpa gerava um juízo de reprovabilidade da conduta o que se altera no direito contemporâneo. Isso porque, para o autor, “a culpa psicológica que deu base à responsabilidade subjetiva, desde sua estruturação como categoria jurídica, deu lugar ao que hoje se denomina culpa normativa”.

Ao passo que a responsabilidade objetiva, eminente legal, possibilita a reparação de um dano cometido sem culpa, se satisfazendo apenas com o dano e o nexo de causalidade. Nesses casos, fala-se em culpa prescindível, posto que a responsabilidade se funda no risco.

Cabe reiterar, que é indispensável a relação de causalidade, entre a ação e o dano. Isso, pois exclui-se a culpa como requisito da responsabilização, mas não a relação lógica de causalidade entre uma conduta e um dano sobre o qual se deseja imputar o dever de indenizar. Assim, admite-se a existência de algumas excludentes de responsabilização pautadas no rompimento do nexo de causalidade, mesmo em relações abarcadas pela objetificação da responsabilidade, o que será aprofundado em momento oportuno.

Nesse sentido Gonçalves[226] acrescenta que responsabilidade objetiva se justifica pela teoria do risco, já que quem exerce alguma atividade, especialmente econômica, e cria um risco de dano para terceiros deve ser obrigada a repará-lo, ainda que sua conduta seja isenta de culpa. Deslocando os holofotes da culpabilidade para o “risco-proveito”.

Desse modo, a responsabilidade objetiva não substituiu a subjetiva, ficando circunscrita aos seus justos limites, posto que o próprio Código Civil brasileiro se filiou à teoria subjetiva, conforme disposição expressa do art. 186. Este que, por sua vez, erigiu o dolo e a culpa como fundamentos para a obrigação de reparar o dano.

A responsabilidade civil por muito tempo teve como fundamento a culpa, porém esta tornou-se insuficiente para “atender às imposições do progresso, cumprindo ao legislador

---

[225] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 jan. 2024.

[226] GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 18 ed. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

fixar especialmente os casos em que deverá ocorrer a obrigação de reparar, independentemente daquela noção”[227].

Contudo, algumas cautelas precisam ser observadas para a adequada aplicação do ordenamento jurídico vigente. De modo que a funcionalidade das normativas que optaram pela aplicação da responsabilidade objetiva seja mantida, sem disfunções sistêmicas.

Avançando na temática, cabe a realização de um aprofundamento da responsabilidade civil sob a perspectiva da proteção de dados por meio das disposições normativas trazidas pela lei nº 13.709 de 2018.

3.2.2 A responsabilidade civil na LGPD

Ab initio, em linhas gerais e sucintas, entende-se por responsabilidade civil o dever de reparação dos danos causados em decorrência da violação de um dever jurídico preexistente, quer seja de natureza contratual ou não. Assim, o Direito brasileiro possui um sistema de tutela que resguarda os que sofrem determinado dano, impondo ao autor do ato que deu causa ao prejuízo o dever de reparar.

Assim, em resumo ao tópico anterior, é possível estabelecer a responsabilidade civil como consequência dos danos causados em decorrência de culpa[228], segundo o qual quem, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito propriamente, conforme descrito no art. 186 do Código Civil. Como também, esta pode decorrer da determinação legal, a exemplo do fato da coisa, do abuso de direito e do risco da atividade, que corresponde à denominada responsabilidade objetiva.

Diante das disposições supramencionadas, grandes doutrinadores, como Gisela Sampaio e Rose Melo Vencelau Meireles[229], aderiram ao entendimento de que a LGPD adotou claramente a teoria subjetiva da responsabilidade civil, devendo haver a prova da conduta culposa do agente de tratamento na ocasião do dano ainda que,

---

[227] PEREIRA. Caio Mário da Silva. **Instituições de Direito Civil**. Rio de Janeiro: Forense, 2022. v.3.
[228] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 29 maio 2024.
[229] GUEDES, Gustavo Siqueira da Costa; MEIRELES, Roberta Motta Veloso. **Término do tratamento de dados.** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Maria de Fátima. Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora RT, 2019, p. 236.

excepcionalmente, a depender do tipo de tratamento, seja aplicável a cláusula geral de responsabilidade pelo risco constante do parágrafo único do art. 927 do Código Civil.

As autoras trazem, por meio do artigo “Término do Tratamento de Dados”[230], uma disposição interessante sobre o tema. Segundo as quais, a lógica da responsabilidade objetiva é outra, posto que não caberia discutir cumprimento de deveres por meio dessa abordagem, sendo tal discussão inerente à análise de culpa ou não do agente.

Desse modo, entendem, por meio de uma interpretação sistemática desta norma, que mesmo a LGPD não dispondo explicitamente quanto à natureza da responsabilidade dos agentes de tratamento de dados, o regime adotado por este diploma foi o da responsabilidade subjetiva.

Outrossim, entendem que os artigos que tratam de standards de conduta a serem seguidos pelos agentes de tratamento de dados para a segurança, sigilo, boas práticas e governança de dados, também são tidos, pelas autoras em questão, como fundamento para o reconhecimento da natureza em comento.

Nesse diapasão, dispõem, em complementação ao elucidado anteriormente, que na análise das exceções do artigo 43, da LGPD, o inciso II pareceria indicar a adoção de uma excludente tipicamente relacionada às hipóteses de responsabilidade civil subjetiva. Principalmente por estatuir que não serão responsabilizados se não houver violação dos preceitos trazidos na legislação de proteção de dados. Portanto, não haveria obrigação de indenizar quando o agente de tratamento de dados demonstrar que observou todo o mencionado standard e, se o incidente ocorreu, não foi em razão de sua conduta culposa.

Por mais que a excludente supra possua um peso significante para a presente análise, cabe ressaltar, também, as relevantes disposições trazidas nos demais incisos do artigo em comento. Estes que, por sua vez, trazem em seu bojo questões importantes para a resolução dos casos concretos. Haja vista que delineiam a exclusão da responsabilidade para os casos de ausência do nexo causal, enquanto não realizaram o tratamento de dados pessoais que lhes é atribuído, e quando o dano for decorrente da culpa exclusiva do titular dos dados ou de terceiros.

Em antítese, cabe ressaltar que outros grandes doutrinadores adotaram uma percepção diversa da outrora suscitada. Exemplos evidenciam-se com Danilo Doneda e

---

[230] GUEDES, Gustavo Siqueira da Costa; MEIRELES, Roberta Motta Veloso. **Término do tratamento de dados.** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Maria de Fátima. Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora RT, 2019, p. 236.

Laura Mendes[231], os quais entendem que se trata, em verdade, de responsabilidade civil eminentemente objetiva.

Ora, para os autores o tratamento de dados representa um risco intrínseco, na medida em que há uma potencialidade danosa significativa em caso de violação dos direitos dos titulares. Assim, a responsabilidade já se fundaria na própria potencialidade do dano, ante a natureza do direito tutelado, enquanto personalíssimo e fundamental, e da atividade tida como de risco, posto a forma de operacionalização do tratamento.

Propondo uma análise sistêmica, vislumbram uma projeção interpretativa conjugada do art. 42 da LGPD com o disposto no art. 927 do Código Civil, o qual delineia em seu parágrafo único que haverá obrigação de reparar o dano, independentemente de culpa, quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. Assim, o mencionado risco atuaria como base para o estabelecimento de critérios próprios de imputação oriundos do incumprimento dos parâmetros de segurança estabelecidos pela lei vergastada.

Nesse interim, trazendo para a presente pesquisa, considerando que os dados virtuais de cunho sensível em saúde serão amplamente coletados e tratados em um ambiente hospitalar, posto a dinâmica da própria atividade, os riscos inerentes ao acesso indevido a tais parecem evidentes.

Caitlin Mulholland[232] acrescenta que, com base na redação do artigo 44 da LGPD, surge o questionamento sobre a possibilidade do legislador ter inaugurado um regime de responsabilidade civil diverso daquele adotado no artigo 42, LGPD. Haja vista que enquanto este último dispositivo impõe a obrigação de indenizar "em razão do exercício de atividade de tratamento de dados pessoais", o artigo 44 e seu parágrafo único da presente normativa determinam a obrigação de indenizar caso haja tratamento irregular de dados pessoais.

A autora elucida que o legislador aparenta querer identificar, nessa hipótese, acontecimentos que se relacionam ao risco inerente ao desenvolvimento da atividade de

---

[231] MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 555, 2018. Disponível em: https://www.revistadedireitodoconsumidor.com.br/. Acesso em: 05 jun. 2024.

[232] MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *In:* MARTINS, Gustavo. M.; ROSENVALD, Nelson. (Org.). **Responsabilidade civil e novas tecnologias**. 1ed. Belo Horizonte: Editora Foco, 2020, v. 1, p. 109-124. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 15 nov. 2023.

tratamento de dados. Quer seja por meio de vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados ou por meio das demais situações danosas que decorrem especificamente de incidentes de segurança. Portanto, aponta que, por meio dessa análise, tais “riscos devem ser necessariamente situados como intrínsecos à atividade de tratamento de dados”, ou seja, em última análise, devem ser considerados como hipótese de fortuito interno.

Assim, não caberia afastar a obrigação dos agentes de tratamento da indenização pelos danos causados em decorrência dos incidentes, já que tais se caracterizam por serem “quantitativamente elevados e qualitativamente graves”, posto que atingem direitos difusos. O que, conforme a autora, já justificaria a adoção da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo.

Ademais, Cavet, Faleiros e Nogaroli acrescentam que o paciente, enquanto usuário final, se enquadra no conceito de consumidor, haja vista que atua como destinatário final do serviço prestado, consoante a exegese do art. 2º do CDC. Sendo, os demais partícipes dessa relação complexa, os fornecedores de serviços, os quais assumirão os ônus decorrentes desse enquadramento.

Complementando, aliás, que os provedores de aplicações de internet não respondem por atos de terceiros que sejam meros usuários desses serviços, embora entendam que tais passem a responder, de forma objetiva, caso intervenham na comunicação, “dando-lhe origem, escolhendo ou modificando o conteúdo ou selecionando o destinatário”[233].

Isto posto, as autoras entendem que atentaria à dinâmica das relações sociais admitir a hipótese em que o titular de dados arque com todos os danos, correlatos à esfera de sua personalidade. Diante do exposto, não seria forçoso admitir, ao menos enquanto regra, a responsabilidade objetiva conferida aos agentes responsáveis pelo tratamento dos dados.

Contudo, cabe abrir uma divergência. Por um lado, parece convincente a arguição de que se trata de uma responsabilidade objetiva, inclusive por mostrar-se como uma prestação de serviço voltada para o armazenamento e a segurança de dados, estes

[233] FALEIROS JÚNIOR, José Luiz de Moraes; NOGAROLI, Ricardo; CAVET, Carlos Alexandre. Telemedicina e proteção de dados: reflexões sobre a pandemia da COVID-19 e os impactos jurídicos da tecnologia aplicada à saúde. **Revista dos Tribunais** [recurso eletrônico]. São Paulo, n. 1016, jun. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/37577. Acesso em: 26 out. 2023.

inseridos na macro noção de tratamento. Requerendo, pois, em caso de vazamento ou violação a dados, apenas a demonstração do nexo causal e da existência do dano.

Por outro lado, não parece adequada a concepção da invasão de sistemas e bases de dados por terceiros como um fortuito interno a justificar a manutenção do processo de responsabilização. Sobre esta disposição cabe um aprofundamento próprio, constando não apenas a adequada distinção entre vazamento e violação de dados, mas também disposições inerentes ao próprio sistema consumerista.

Assim, assume-se que a culpa prescinde de demonstração, mas a comprovação da adequada existência de um nexo causal intacto se mostra extremamente devida, com respaldo na própria teoria geral da responsabilidade civil.

Abordar de modo genérico e abstrato sobre a existência de risco inerente ao desenvolvimento da atividade de tratamento de dados, sem abarcar a existência de standards de segurança, padrões normativos e o estado da arte da tecnologia, ocasionaria uma imposição de indenização sem a observância dos seus pressupostos e critérios dogmáticos. O que para Tepedino “representa, a médio prazo, o colapso do sistema, uma violência contra a atividade econômica e um estímulo ao locupletamento indevido”[234].

Por hora, faz-se necessária uma atenta análise do artigo 43 da LGPD, o qual respalda a presente disposição. Essa normativa funda-se na expressa exclusão da responsabilização diante da ocorrência devidamente provada de fato exclusivo de terceiro ou do titular dos dados, abordando, desse modo, hipóteses de rompimento do nexo causal.

Nos casos em que a obtenção do dado supramencionado decorreu, de modo comprovado, do uso ardiloso dos instrumentos do terceiro absolutamente desconectado à prestação do serviço de armazenamento de dados de saúde no meio virtual, haveria a possibilidade de aplicação dessa disposição excludente de responsabilização.

Isso, tendo o hospital adotado não apenas as disposições concernentes na LGPD, como também as tecnologias mais avançadas, considerando o estado da arte dos aparatos de telecomunicação, na época da interferência. O que evidencia-se por meio da leitura combinada dos artigos 46 e 44 da LGPD.

---

[234] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

Essa análise sistemática dos dispositivos supramencionados orienta sobre o que seria um tratamento irregular a ferir o dever de segurança na tutela do dado. Dispondo, mais, que a irregularidade em questão deve ser analisada sob a ótica de determinadas circunstâncias legalmente previstas. Dentre as quais, o modo de realização do tratamento dos dados, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Evidenciando de modo ainda mais contundente a existência da delimitação legal dada ao que seria risco interno ou externo na prática do tratamento de dados. A não adoção dos parâmetros normativos e técnicos existentes, parece elevar de modo considerável o risco inerente à prática do tratamento de dados. O que configura um evidente risco interno da prática.

Diferente da perspectiva trazida pelo surgimento posterior de um mecanismo de acesso indevido a uma estrutura de armazenamento de dados altamente respaldada pelos parâmetros de segurança existentes quando da realização do tratamento dos dados pessoais do indivíduo.

Cabe, assim, a menção ao parágrafo único do art. 44 da LGPD, segundo o qual responde pelos danos decorrentes da violação da segurança dos dados o controlador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Este dispositivo legal dispõe em seu parágrafo primeiro que a autoridade nacional poderá delimitar sobre padrões técnicos mínimos. Especialmente considerando critérios como “a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia”. Destacando, mais, um cuidado especial com os dados pessoais sensíveis, sempre observando a aplicação dos princípios previstos no caput do art. 6º da lei outrora analisada.

Cabendo recordar a exaustiva disposição quanto necessidade que a instituição possui de notificar de modo claro, amplo e inequívoco o paciente, quanto aos riscos inerentes a essa modalidade de atendimento. Adquirindo, assim, o consentimento livre e esclarecido do titular dos dados sensíveis.

Partindo das disposições outrora trazidas, nos casos em que a mencionada invasão por fato de terceiro decorreu, em verdade, de falha na prestação de segurança do serviço ou não fora realizada a notificação adequada dos pacientes quanto aos riscos inerentes ao

canal de atendimento, os agentes do tratamento de respondem solidariamente pelos danos causados (artigo 42, §1º, II da LGPD)[235].

Portanto, a simples intervenção irregular do terceiro, por si só, não exime o agente dos dados da responsabilidade que lhe cabe na medida da sua participação no evento danoso. Posto que precisa ser evidenciada a ação exclusiva do terceiro, para que haja a isenção na responsabilização.

A presente percepção quanto à mitigação da responsabilidade objetiva mostra-se como incentivo positivo ao incremento dos investimentos empresariais aos parâmetros de segurança trazidos em realização às normas da LGPD. Isso porque, a partir do momento que a necessidade de reparação ao dano causado só surge mediante prova da culpa e não da mera ocorrência do fato danoso, as empresas passam a investir cada vez mais em aparatos de segurança avançados, buscando se salvaguardarem de quaisquer prejuízos decorrentes da ação de terceiros completamente estranhos àquele vínculo profissional.

Nessa esteira, transcendendo as diretrizes de culpa ou não, um outro fator relevante para a responsabilização é o nexo causal entre a ocorrência do dano e a ação do agente. Haja vista que, em recente julgado, a 3ª turma do STJ entendeu que não haveria responsabilidade da plataforma no caso em que o fraudador não usufrui dos instrumentos por ela disponibilizados.

No vertente caso, a fraude ocorrera por fora dos limites de atuação disponibilizados pela plataforma, Mercado Livre, para praticar a fraude. Desse modo, o ocorrido não poderia ser qualificado como uma falha no dever de segurança. Bem como, não teria ocorrido uma divulgação indevida de dados pessoais, nem mesmo violação do dever de informar. Resta ausente, assim, a falha na prestação dos serviços.

Ademais, além da demonstração do nexo causal, o juiz Mario Sergio Leite, da 2ª vara Cível de Osasco (SP), em recente decisão[236], entendeu que haveria a necessidade de demonstração do dano para a configuração da necessidade de reparação. O magistrado entendeu que o vazamento de dados por si só não acarreta consequências gravosas à imagem, personalidade ou dignidade, sendo preciso provar que houve dano concreto, posto

---

[235] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

[236] SANTOS, Ricardo. Prejuízo por vazamentos de dados deve ser provado para justificar dano moral. **Consultor Jurídico**. 2021. Disponível em: https: https://www.conjur.com.br/2021-jun-22/vazamento-dados-gera-indenizacao-dano-for-provado. Acesso em: 11 out. 2023.

que o prejuízo decorrente da falha da empresa que coletou os dados teria sido apenas potencial. Essa seria, portanto, mais uma questão passível de análise posterior.

De fato, conforme as disposições outrora mencionadas, não se trata de um desafio simples, de modo que tais disposições ainda serão objeto de profundas pesquisas no que tange à aplicação da LGPD. Assim, caberá a atuação diligente da Autoridade Nacional de Proteção de Dados para preencher as lacunas legais e editar instruções necessárias à preservação dos direitos individuais e garantia da confiança dos indivíduos na coleta de dados, bem como um esforço dos Tribunais pátrios para estabelecer as balizas interpretativas da Lei.

3.2.3 Responsabilidade hospitalar e o Código de Defesa do Consumidor - CDC

Diante do que outrora foi analisado, traz-se a presente pesquisa para a perspectiva do Código de Defesa do Consumidor. Posto que, retomando as análises de Cavet, Faleiros e Nogaroli[237], o paciente, enquanto usuário final, se enquadra no conceito de consumidor, haja vista que atua como destinatário final do serviço prestado, consoante a exegese do art. 2º do CDC. Cabendo aos demais partícipes dessa relação complexa, a função de fornecedores do serviço, os quais assumirão os ônus decorrentes desse enquadramento.

Outrossim, trazendo para o ambiente hospitalar, retomam-se algumas lições de Kfouri[238] como ponto de partida para as análises subsequentes. Uma perspectiva inicial está conectada à complexidade demasiada da responsabilidade de uma estrutura hospitalar, posto a existência de diversas atividades distintas sendo desempenadas em um mesmo espaço.

Dispor de uma maneira genérica sobre todas as prestações realizadas pelo hospital esbarraria em pressupostos falaciosos. Não se pode utilizar dos mesmos pontos de partida para análise da responsabilidade da instituição quanto a serviços inerentes a prestações paramédicas, extramédicas ou ao atendimento médico em si.

---

[237] FALEIROS JÚNIOR, José Luiz de Moraes; NOGAROLI, Ricardo; CAVET, Carlos Alexandre. Telemedicina e proteção de dados: reflexões sobre a pandemia da COVID-19 e os impactos jurídicos da tecnologia aplicada à saúde. **Revista dos Tribunais** [recurso eletrônico]. São Paulo, n. 1016, jun. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/37577. Acesso em: 26 out. 2023.

[238] KFOURI, Maurício Zanoide de Moraes. **Responsabilidade Civil dos Hospitais - Código Civil e Código de Defesa do Consumidor.** São Paulo: Thomson Reuters Revista dos Tribunais, 2022. RB-1.1. Ebook. ISBN 9786559910489. Disponível em:https://nextproview.thomsonreuters.com/launchapp/title/rt/monografias/105155050/v5/page/RB-1.1%20. Acesso em: 22 nov. 2023.

Assim, cabe direcionar a presente análise para a responsabilidade da instituição quanto a atividade de guarda dos prontuários dos pacientes, a qual se situa na perspectiva dos serviços extramédicos. Esta que, nitidamente, se insere na esfera empresarial do serviço prestado pelo hospital, configurando, pois, a aplicação do Código de Defesa do Consumidor.

Segue-se, pois, a uma análise dos pressupostos e normativas trazidos pelo CDC visando uma análise contundente sobre o sistema de responsabilização aplicável ao presente estudo. Inicialmente, uma premissa básica do sistema consumerista versa que o consumidor é a parte vulnerável das relações de consumo.

Assim, o Código pretende restabelecer o equilíbrio entre os protagonistas de tais relações, criando princípios e regras em que se sobressai não mais a igualdade formal das partes, mas a vulnerabilidade do consumidor, o qual deve ser protegido. Nesse cenário, surge um contexto de responsabilização objetiva, no qual a demonstração de culpa do fornecedor torna-se irrelevante para o processo indenizatório.

Para uma adequada tutela deste elo mais vulnerável, acabam sendo limitadas as excludentes de responsabilidade invocáveis pelo agente, facilitam-se os mecanismos de defesa dos direitos do consumidor, inclusive com a inversão do ônus da prova no processo civil[239].

Passadas essas noções introdutórias, cabe uma análise mais profunda sobre as disposições inerentes à prestação de serviços no sistema consumerista e suas aplicações à vertente pesquisa. Parte-se do artigo 14 do CDC, o qual estabelece que o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

Respalda-se, pois, a mencionada aplicação da responsabilidade objetiva ao caso, porém cabe uma atenção específica para a ideia de defeito na prestação, a qual fora inserida pelo Código em análise. Inicialmente, ressalta-se que trata de uma categoria objetivamente auferível, considerando, inclusive, o contexto da sua inserção.

---

[239] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 29 maio 2024.

Depois, cabe elucidar que tal defeito não deve ser tido como pressuposto de culpa[240], mas como inerente na concepção de falha na prestação do serviço, uma característica adicional incluída pelo legislador, a qual deve ser observada no processo de responsabilização.

Nesse ponto, o CDC[241] expõe o conceito de serviço defeituoso como sendo o que não fornece a segurança que o consumidor dele pode esperar. Contudo, a normativa estatui a necessária observância de algumas circunstâncias relevantes, para que o defeito seja adequadamente aferível. Dentre as quais: o modo em que o serviço é fornecimento, o resultado e os riscos que razoavelmente dele se esperam e a época em que foi fornecido.

Desse modo, o Código de Defesa do Consumidor tutela a legítima expectativa do consumidor atinente à segurança e à adequação dos produtos e serviços, mas faz recortes relevantes para que a perspectiva adotada não ocasione disfunções sistêmicas.

Destacam-se algumas considerações sobre a vertente questão, das quais cabe mencionar que a expectativa referente à segurança da prestação deve vincular-se à forma que fora realizada, considerando os métodos e técnicas adotados e a adequação destes aos parâmetros do setor em que se situam. Disposição que se vincula à própria noção do que seria um risco adequadamente esperado ou razoável.

Outrossim, evidencia-se uma preocupação do CDC com a época em que o serviço fora fornecido. O que permite uma análise de adequação sob uma perspectiva temporal da prestação. Aspecto especialmente relevante em um século marcado por mutabilidades rápidas e significativas sobre os setores. Disposição que deve ser analisada em sintonia com o art. 44 da LGPD que associa a segurança que o titular pode esperar do tratamento de dados pessoais às técnicas disponíveis à época em que foi realizado, o que limita e especifica a ideia de defeito.

---

[240] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[241] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 29 maio 2024.

Assim, cabe destacar algumas lições de Tepedino[242], o qual levanta uma relevante discussão sobre o incremento dos riscos no meio digital, e ilustra o cenário abordado com um exemplo categórico no qual:

> (...) Tanto que, neste caso, ainda que o consumidor adquira o melhor programa antivírus disponível no mercado, não terá a legítima expectativa de que seus documentos estarão inteiramente invulneráveis a todo e qualquer ataque hacker, o que é evidenciado pelas permanentes atualizações do software voltadas justamente a combater os novos vírus, que se desenvolvem de modo permanente.

Passa-se, então, a uma projeção quanto ao denominado risco do desenvolvimento. Este que, para Tepedino[243], afasta a configuração do defeito do serviço e, consequentemente, o dever de indenizar. Já na perspectiva de Miragem[244] os riscos do desenvolvimento em questão encontram-se sob a égide da responsabilidade do fornecedor, posto que não poderia ser confundida como hipótese de exclusão de responsabilidade, sob pena de subverter a sistemática do CDC. Contudo, concluir pela inaplicação da hipótese de exclusão de responsabilidade contraria as disposições expressas no Código.

Ademais, apesar de aparentar, sob uma óptica inicial, uma salvaguarda ao elo mais vulnerável da relação, garantindo algum tipo de compensação financeira por toda e qualquer violação a dado, em verdade estaria atuando como respaldado ao agravamento à tutela dos direitos da personalidade do consumidor, o que efetivamente subverte a sistemática do CDC.

Para tanto, cabe uma menção à análise econômica do direito, a qual está fundada, para Mackaay[245], na premissa de que “as normas jurídicas devem ser julgadas à luz das estruturas de estímulos que estabelecem e das consequentes mudanças comportamentais adotadas pelos interessados em resposta aos estímulos”. Busca-se, pois, a análise das consequências associadas a determinadas medidas.

A adoção das políticas instituídas pela LGPD, por si só, já onerou significativamente o orçamento das empresas de diversos portes que atuam, em alguma medida, com o

---

[242] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[243] *Ibid.,* p. 158.

[244] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 15 jan. 2024.

[245] MACKAAY, Ejan. ROUSSEAU, Stefan. **Análise Econômica do Direito**. São Paulo: Editora Atlas, 2015. p. 665.

gerenciamento de dados, o que se mostrou como extremamente relevante para o estabelecimento de um padrão de segurança condizente com a relevância dos dados tratados. A normativa estabeleceu um compilado de parâmetros que, em caso de não observância, ocasionam diversas consequências nas mais variadas esferas de responsabilidade.

Entretanto, para além dos parâmetros normativos, existem parâmetros técnicos adicionais que podem robustecer o protocolo de segurança digital. O que também está associado a custo extra para adequada tutela dos dados no ambiente virtual. Assim, parece interessante, sob a própria perspectiva sistêmica, a promoção de estímulos legais às boas práticas em segurança de dados.

O que se evidencia como oposto à a imposição de indenização sem a observância dos seus pressupostos, que, nas palavras de Tepedino[246], “poderia ocasionar o colapso do sistema, uma violência contra a atividade econômica e um estímulo ao locupletamento indevido.” Isso, porque a mencionada inobservância pode alimentar a ponderação quanto a riscos que valeriam, economicamente, a pena serem assumidos.

Já que, independentemente da adoção dos melhores protocolos, as empresas arcariam com a manutenção de processos informacionais no maior padrão de proteção possível, adotariam uma mão de obra adequadamente especializada e, em caso de violação a dados, ainda arcariam com vultuosas indenizações e incomensuráveis perdas financeiras e reputacionais.

Inclusive, de acordo com pesquisa realizada pela Kaspersky Lab[247], a qual fora disponibilizada 2018, o custo médio que um incidente de segurança gera para as empresas, considerando o período de análise entre março de 2017 e fevereiro de 2018 atingiu 1,23 milhão de dólares, representando índice 24% maior que o período imediatamente anterior (2016-2017) e 38% maior em comparação ao período de 2015-2016. Quando o recorte é feito para pequenas e médias empresas, a perda por incidente acaba sendo estimada em 120.000 dólares, ocasionando um acréscimo na ordem de 32.000 dólares com relação ao ano antecedente.

---

[246] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

[247] KASPERSKY. **What is the cost of data breach**? In: Kaspersky blog. s.l: 2018. Disponível em: https://www.kaspersky.com/blog/economics-report-2018/22486/. Acesso em: 11 jan. 2024.

No Brasil, conforme outrora exposto, não existe consenso a respeito do assunto. A busca pela conciliação entre as necessidades de desenvolvimento e aprimoramento da ciência com a legítima expectativa de segurança do consumidor, torna a questão ainda mais controvertida. Ao contrário, na União Europeia, o art. 7º, “e”, da Diretiva 85/374, prevê o risco de desenvolvimento como excludente de responsabilidade[248].

Esta conjuntura em nada se confunde com a abordagem do art. 23 do mesmo Código, segundo o qual “a ignorância do fornecedor sobre os vícios de qualidade por inadequação dos serviços não o exime de responsabilidade”. Posto que, fala-se da existência de um vício prévio desconhecido pelo fornecedor quanto a inadequação da prestação realizada, diferente seria o surgimento de uma violação nova não atrelada a nenhum vício preexistente.

Trazendo para uma vertente de proteção de dados, um vício de qualidade na segurança da informação ocasionado pelo uso de um software inadequado ou uma autenticação mal feita, mesmo que ignorados pelo fornecedor, em nada se confunde com a violação, por um mecanismo completamente novo, de um sistema que fazia a adoção dos melhores padrões de segurança do momento.

Um outro ponto relevante nessa equação é a disposição final do artigo 14 do CDC, o qual fundamenta a necessidade do repasse de informações suficientes e adequadas sobre sua fruição e riscos do serviço, os quais devem ser razoavelmente conhecidos pelo consumidor.

Comunicação esta que se encontra vinculada à noção de legítima expectativa de segurança, já que os riscos da prestação de serviço presumem-se conhecidos pelo fornecedor e devem ser repassados ao consumidor. Conforme discussões anteriores realizadas no tópico do consentimento devidamente informado.

---

[248] O produtor não é responsável nos termos da presente diretiva se provar “que o estado dos conhecimentos científicos e técnicos no momento da colocação em circulação do produto não lhe permitiu detectar a existência do defeito”. O art. 15 da mesma Diretiva 85/374, por sua vez, em sua alínea “b”, assevera: “Cada Estado-membro poderá: (...), Não obstante o previsto na letra e) do art. 7º, manter ou, sem prejuízo do procedimento definido na segunda parte do presente artigo, dispor em sua legislação que o produtor seja responsável mesmo se demonstrar que, no momento em que pôs o produto em circulação, o estado dos conhecimentos técnicos e científicos não permitia detectar a existência do defeito.
MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 11 jan. 2024.

Passadas essas discussões, cabe adentrar nas disposições concernentes ao art. 14, § 3º, do CDC, o qual determina que o fornecedor de serviços só não será responsabilizado quando provar a inexistência do defeito, no caso de a prestação de serviço ter ocorrido, ou a culpa exclusiva do consumidor ou de terceiros.

Um norte inicial quanto às hipóteses previstas como excludentes da responsabilidade está atrelado a atuação destas diretamente sobre o nexo de causalidade, rompendo-o e, assim, afastando o dever de indenizar. Outro ponto relevante para a continuidade na discussão da temática vincula-se à existência de concorrência ou não entre o comportamento da vítima ou de terceiro e o vício na prestação do serviço.

Para que ocorra a adequada exclusão da responsabilidade, a ação da vítima ou do terceiro deve ser exclusiva e efetiva para a concretização do dano. Nos casos de comprovada concorrência entre causas, resta-se apenas mitigada a amplitude da responsabilização, já que o nexo causal persiste quanto à ação do controlador e a ocorrência do dano, o que será posteriormente aprofundado.

Passados os nortes iniciais, cabe evidenciar que o código consumerista estabelece três excludentes de responsabilidade ao fornecedor de serviços. A primeira, a qual versa sobre a inexistência do defeito na prestação do serviço, já fora mencionada nas discussões anteriores. Cabendo, pois, um enfoque nas excludentes quanto a culpa exclusiva do consumidor ou de terceiros.

No que concerne à responsabilidade por fato de terceiro, cabe um relevante recorte. Para que a excludente seja aplicada ao caso concreto, o responsável pelo dano, que para o vertente caso é ocasionado pelo acesso indevido a dado sensível, não pode ter nenhuma conexão com a instituição controladora dos dados.

Isso porque, qualquer vínculo evidenciado entre o terceiro e o hospital resultaria na aplicação do chamado fortuito interno[249], no qual o agente que deu causa à situação indesejada estaria ligado à empresa prestadora do serviço. Sendo, pois, um risco ligado à atividade desenvolvida pelo agente. Não sendo passível de aplicação da excludente de responsabilidade, posto a impossibilidade do rompimento do nexo de causalidade na vertente conjuntura.

---

[249] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

Assim, para que efetivamente se aplique o fato de terceiro, é necessária a ocorrência de um fortuito externo, no qual não se liga a empresa ao agente causador do dano por nenhum vínculo ou conexão. O que rompe, efetivamente, com o nexo de causalidade. De modo a eximir o agente do dever de indenizar.

Nesse ponto, existe o enquadramento da atuação dos hackers. Caso que isenta a responsabilidade civil do controlador dos dados nos casos de não ocorrência de defeito no tratamento prestado. Temática esta que será retomada em tópico posterior.

Já o fato exclusivo da vítima representa a ocorrência do "evento que se identifica como causa necessária de um dano sofrido por ela, e cuja realização só possa ser a ela imputável"[250]. Nesse ponto, o dano ocorreu não em razão da atividade do fornecedor do serviço, mas em razão de comportamento exclusivo da própria pessoa que sofreu o dano.

Cabendo ressaltar a necessidade do fato da vítima ter sido a causa necessária do dano, afastando as demais causas possíveis, inclusive afastando qualquer conduta ou a atividade do agente "de que se investigue eventual responsabilidade"[251]. A exemplo da disponibilização, pelo próprio titular dos dados, de seu login e senha de acesso ao sistema de determinada instituição hospitalar a terceiro que julgava confiável, mas que, após o fato, tal passou a usar indevidamente das informações obtidas ou repassou o acesso a quem não tinha autorização a tê-lo.

Assim, evidencia-se que o exame do nexo causal é imprescindível para o processo indenizatório. Inclusive, aplicável na identificação quanto a existência de alguma hipótese de exclusão do dever de reparar, quer seja decorrente de fato exclusivo de terceiro ou da vítima. Referenciando, assim, às análises subsequentes.

---

[250] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 11 jan. 2024.

[251] *Ibid.,* p. 47.

4 DANO POR ACESSO INDEVIDO A DADOS SENSÍVEIS DE SAÚDE E A DIMENSÃO INDENIZATÓRIA

4.1 DANO

4.1.1 Distinção entre acesso indevido e vazamento de dados

Para uma melhor compreensão do outrora exposto, urge distinguir o vazamento de dados do acesso indevido, os quais se confundem sob a vertente de diversos doutrinadores. Inicialmente, cabe importar dois conceitos relevantes, o "*data leak*" e o denominado "*data breach*"[252].

O primeiro ocorre quando informações confidenciais são acidentalmente ou intencionalmente expostas a indivíduos ou organizações que não possuem autorização para acessá-las. De modo que os dados confidenciais são acidentalmente expostos fisicamente, na Internet ou de qualquer outra forma, permitindo que criminosos cibernéticos obtenham acesso não autorizado aos dados confidenciais sem esforço[253].

Normalmente, o incidente em comento está atrelado a erros humanos, como envio de informações confidenciais para um e-mail incorreto ou por meio de falhas nos sistemas de armazenamento de dados. A exemplo do vazamento de senhas do Ministério da Saúde, o qual deixou exposto na internet dados pessoais e médicos de ao menos 16 milhões de brasileiros que tiveram diagnósticos suspeitos ou confirmados de COVID-19[254].

Cabe mencionar, também, a seguinte jurisprudência do Tribunal de Justiça do Estado de São Paulo que retrata a dinâmica do vazamento de dados outrora discutida:

> APELAÇÕES CÍVEIS. DANOS MORAIS. DANOS MATERIAIS. DIVULGAÇÃO DE PRONTUÁRIO MÉDICO. HIV. Dados médicos do autor disponibilizados ao público no site (...) a simples inserção de seu CPF e sua data de nascimento, informações essas de fácil acesso. **Ausência de senha de acesso que torna a informação, na prática, pública.** O vazamento do prontuário médico do requerente (fls. 31/35), ao indicar ser ele portador do vírus do HIV, gerou situação embaraçosa e degradante

[252] AMORIM, Allex. Diferenças do Data Leak e Data Breach. **Linkedin**, São Paulo, 09 de março de 2023. Disponível em: https://pt.linkedin.com/pulse/diferenças-do-data-leak-e-breach-alex-amorim. Acesso em: 28 dez. 2023.
[253] TUNGGAL. Allan Toh. What is a Data Leak? Stop Giving Cybercriminals Free Access. **UpGuard,** 2023. Disponível em: https://www.upguard.com/blog/data-leak. Acesso em: 26 dez. 2023.
[254] FCQ ADVOGADOS. **Vazamento de dados no Ministério da Saúde expõe informações pessoais de 16 milhões de pacientes.** 2020. Disponível em: https://www.fcqadvogados.com/vazamento-de-dados-no-ministerio-da-saude-expoe-informacoes-pessoais-de-16-milhoes-de-pacientes/. Acesso em: 28 dez. 2023.

> no ambiente de trabalho. A responsabilidade civil objetiva exige apenas a ocorrência do dano, a existência de nexo causal entre a conduta e este dano e a ausência de culpa excludente da vítima (art. 37, § 6º CF). O sigilo dos dados pessoais ganha contornos cada vez mais sensíveis, sendo matéria cada dia mais regulada na seara legislativa. Eventuais vazamentos de dados particulares são evidentes fatos geradores de danos, seja de ordem moral ou material, e o legislador tende a protegê-los, especialmente quando digam respeito aos direitos de personalidade. Art. 5º, X, Constituição Federal, art. 42 da Lei nº 13.709/2018 (LGPD) e art. 4º da Lei 13.787/2018. Danos morais configurados. Quantum indenizatório majorado. Danos materiais não configurados. Ausência de prova de nexo de causalidade entre a exposição dos dados médicos e a efetiva demissão do autor. Honorários advocatícios readequados. Recurso do autor parcialmente provido. Recurso do réu desprovido. TJ-SP - AC: 10168440320208260068 SP 1016844-03.2020.8.26.0068, Relator: Heloísa Martins Mimessi, Data de Julgamento: 05/07/2021, 5ª Câmara de Direito Público, Data de Publicação: 07/07/2021[255] (Grifo meu).

Parte dos casos de vazamentos de dados estão vinculados a erros de baixa complexidade, como nos casos de práticas inadequadas de segurança de dados ou configurações incorretas de *software*, mas que ocasionam danos de proporções significativas. Alguns dos quais podem ser facilmente identificados tanto na esfera patrimonial, como na esfera privada do titular dos dados.

Já outros danos potencialmente gravosos podem ser de difícil comprovação, ao menos inicialmente, em especial no que concerne a impossibilidade de dimensão quanto por quem foram acessados ou como serão utilizados. Os riscos variam desde possíveis extorsões e fraudes até a venda de dados na *Dark Web*.

Assim, cabe reiterar que um vazamento de dados não se confunde com a noção pura de acesso indevido, apesar de ser evidente que a exposição desses dados confidenciais pode ser usada para agilizar futuras violações de dados. A título exemplificativo, dados roubados publicados em blogs de *ransomware* são classificados como vazamentos de dados[256], posto que podem ser usados para comprometer redes de TI com menos esforço.

Por outro lado, um *Data Breach* ocorre quando informações confidenciais são acessadas por indivíduos ou organizações não autorizados[257], tratando, pois, de uma

---

[255] SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. 5ª Câmara de Direito Público**. Apelação Cível nº 10168440320208260068 SP**. Danos Morais. Danos Materiais. Divulgação De Prontuário Médico. Hiv. Relatora: Heloísa Martins Mimessi. 07 de julho de 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2097727220/inteiro-teor-2097727224. Acesso em: 11 nov 2023.

[256] TUNGGAL. Allan Toh. What is a Data Leak? Stop Giving Cybercriminals Free Access. **UpGuard,** 2023. Disponível em: https://www.upguard.com/blog/data-leak. Acesso em: 26 dez. 2023.

[257] AMORIM, Allex. Diferenças do Data Leak e Data Breach. **Linkedin**, São Paulo, 09 de março de 2023. Disponível em: https://pt.linkedin.com/pulse/diferenças-do-data-leak-e-breach-alex-amorim. Acesso em: 28 dez. 2023.

violação dos dados. Durante essa ocorrência, a segurança dessas informações é violada, as deixando disponíveis para pessoas, usualmente, mal-intencionadas.

O incidente de Segurança em questão é mais comum em ataques cibernéticos, no qual *hackers* invadem sistemas de armazenamento de dados e roubam informações valiosas, que podem ser relativas a dados de saúde ou demais questões sensíveis.

Uma violação de dados[258], portanto, é um incidente em que informações são roubadas ou retiradas de um sistema sem o conhecimento ou autorização do proprietário do sistema. Podendo ter efeitos altamente prejudiciais não só para os titulares dos dados, mas também para as empresas[259]. O que fica evidente através de perdas financeiras e dos danos à reputação perante clientes, funcionários e demais membros da sociedade.

Além disso, as organizações também podem estar sujeitas a multas e implicações legais decorrentes de regulamentações de dados e privacidade cada vez mais rigorosas, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei de Privacidade do Consumidor da Califórnia (CCPA).

Nesse sentido, o GDPR, em seu art. 4.º, item 12, traz a definição de violação de dados pessoais: “uma violação da segurança[260] que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento”.

Por sua vez, a LGPD, em seu artigo 46, não define vazamento, incidente ou violação de dados pessoais. Adotando, indiretamente, um conceito semelhante[261] ao do GDPR, ao determinar que “os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas”. Tais intercorrências podem envolver destruição, perda, alteração, comunicação ou qualquer forma de tratamento tido por inadequado ou ilícito.

---

[258]HOLMES, David. What is Data Breach? **Fortnet,** 2023. Disponível em:https://www.fortinet.com/resources/cyberglossary/data-breach. Acesso em: 28 dez 2023.

[259]*Ibid.*

[260] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados **(Regulamento Geral sobre a Proteção de Dados).** Jornal Oficial da União Europeia. L 119/1, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 29 maio 2024.

[261] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

Dispondo, mais, quanto ao que seria um tratamento irregular dos dados, consoante o art. 44, *caput,* da LGPD: “quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes”[262].

A distinção dos termos em análise ganha contornos relevantes nos quesitos de responsabilização dos controladores dos dados e na adoção das condutas necessárias para romper com a ameaça. Já que são decorrentes de pressupostos distintos.

Em um *Data Leak,* as organizações devem trabalhar para minimizar o dano da exposição dos dados e tomar medidas para evitar que informações confidenciais sejam acessadas por indivíduos não autorizados. Quanto responsabilidade cível dos controladores, caberia, em linhas superficiais, uma responsabilização nos contornos da LGPD e do CDC pelo não fornecimento da segurança que validamente o titular dos dados esperava, especialmente nos contornos do vazamento por falha no sistema.

Ao passo que, em um *Data Breach*, as organizações devem agir rapidamente para bloquear o acesso de indivíduos mal-intencionados aos dados roubados, identificando e remediando as falhas de segurança que permitiram a invasão e notificar as autoridades e as pessoas afetadas[263].

No aspecto da responsabilização dos controladores dos dados, cabe uma análise mais profunda quanto a real adoção das medidas adequadas para evitar qualquer tipo de intercorrência negativa, sendo averiguada sob uma perspectiva mais analítica. Em sintonia com as discussões anteriormente realizadas.

4.1.2 A noção jurídica de dano por acesso indevido a dados sensíveis de saúde

Uma compreensão mais profunda quanto aos contornos outrora delineados perpassa pela retomada da distinção entre os dados pessoais comuns e os dados sensíveis. Assim, cabe reiterar que os primeiros, para o art. 5º da LGPD[264], são informações

---

[262] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

[263] AMORIM, Allex. Diferenças do Data Leak e Data Breach. **Linkedin**, São Paulo, 09 de março de 2023. Disponível em: https://pt.linkedin.com/pulse/diferenças-do-data-leak-e-breach-alex-amorim. Acesso em: 28 dez. 2023.

[264] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

relacionadas[265] à pessoa natural identificada ou identificável, os quais compõe os atributos e características que tornam o indivíduo singular, o chamado prolongamento pessoal. De modo que, a proteção proposta pela normativa sob análise buscou ser bastante abrangente, especialmente quando estabelece um conceito tão amplo sobre dado pessoal.

Por outro lado, em consonância com exposições anteriores, os dados sensíveis compreendem uma tipologia distinta em decorrência da natureza do seu conteúdo oferecer uma especial vulnerabilidade. Dentre estes, existem os que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surgindo, dessa forma, a razoável preocupação em haver discriminação ou diferenciação de uma pessoa em detrimento de tais aspectos da sua personalidade.

Essa distinção quanto a natureza do dado mostra-se como extremamente relevante para uma adequada dimensão da noção jurídica de dano por acesso indevido a dados sensíveis do paciente. Para melhor vislumbrar a questão sob análise, cabe mencionar a decisão da 2ª Turma do Superior Tribunal de Justiça, em 7 de março de 2023, a qual entendeu que o vazamento de dados pessoais não gera dano moral presumido (*in re ipsa*), "sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações"[266].

A decisão em questão foi proferida nos autos do Agravo em Recurso Especial nº 2.130.619/SP e reformou acórdão do Tribunal de Justiça de São Paulo que havia condenado a empresa Eletropaulo Metropolitana Eletricidade de São Paulo S.A. ao pagamento de indenização por dano moral em decorrência do vazamento de dados pessoais da autora.

Antes de abordar sobre questões inerentes ao dano, ressalta-se que o termo vazamento de dados constante no acórdão se apresenta com uma conotação genérica, sem levar em consideração as distinções outrora mencionadas. Partindo desse

---

[265] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 59.

[266] BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: Maria Edite de Souza. Processual Civil e Administrativo. Indenização por Dano Moral. Vazamento de Dados Pessoais. Dados Comuns e Sensíveis. Dano Moral presumido. Impossibilidade. Necessidade de Comprovação do Dano. Relator: Min. Francisco Falcão, 07 mar. 2023. Disponível em:https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28ARESP.clas.+e+%40num%3D%222130619%22%29+ou+%28ARESP+adj+%222130619%22%29.suce.&O=JT. Acesso em: 03 mar 2023.

pressuposto, passa-se à análise da inaplicabilidade do dano moral presumido (in re ipsa) aos casos de vazamento dos dados pessoais não sensíveis.

Cabendo, inicialmente, dispor sobre algumas premissas que levaram a Corte ao entendimento supra. A primeira seria que o art. 5º, II, da LGPD, dispõe de forma taxativa sobre quais dados podem ser considerados sensíveis, demandando tratamento diferenciado. Considerando, pois, que os demais dados de natureza comum, não íntimos, seriam passíveis apenas de identificação pessoal.

Essa premissa foi questionada por diversos doutrinadores, a exemplo da professora Caitlin Mulholland, a qual entendeu que "não somente o conteúdo dos dados previsto neste inciso merecerão a qualificação como dados sensíveis, podendo abarcar outras situações não previstas"[267]. Evidenciando um contundente *modus operande*, já que mesmo o dado não se mostrando relevante em linhas iniciais, por meio de um processo de tratamento, no qual algumas informações são cruzadas e organizadas, podem ser formados dados específicos sobre determinada pessoa[268].

Para José Henrique de Oliveira Couto[269], a interpretação das hipóteses do art. 5º, II, da LGPD como taxativas mostra-se equivocada. O autor considera que a presente sociedade do risco, do conhecimento, da inovação, da globalização demanda a superação da bifurcação entre as definições de dado sensível e dado pessoal. Fundamentando uma análise à luz do caso concreto para a demonstração da real natureza do dado pessoal.

Ocorre que, conforme pontua Daniele Marcon[270], se um incidente de segurança puder causar risco ou dano relevante, o artigo 48, §1º, I, da LGPD indica que a comunicação a ser encaminhada à autoridade nacional deve descrever a "natureza dos dados pessoais afetados". O envolvimento de dados sensíveis no incidente não seria, para a autora, um requisito para reconhecer o risco ou dano relevante, sendo apenas um elemento da análise.

---

[267] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. São Paulo, **Revista do Advogado**, ano XXXIX, nº 144, nov. 2019, p. 48.

[268] VIOLA, Marcelo; TEFFÉ, Carolina. Tratamento De Dados Pessoais Na LGPD: Estudo Sobre as Bases Legais Dos Artigos 7.º E 11. *In:* DONEDA, Danilo. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 6, p. 131.

[269] COUTO, José Henrique Oliveira. Vazamentos De Dados E Dano Moral 'In Re Ipsa': Comentários Ao Agravo Em Recurso Especial Nº 2.130.619/Sp. **Revista IBERC**, v. 06, n. 02, p. 171-188, mai./ago. 2023. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/52/42. Acesso em: 28 dez. 2023.

[270] MARCON, Daniele Vidal. Dano moral e vazamento de dados: o STJ escreveu certo por linhas tortas? **Consultor Jurídico**, abr. 2023. Disponível em: https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados/. Acesso em: 24 nov. 2023.

Arguindo, mais, que a fronteira entre um dado pessoal "comum" e um "sensível" não possui contornos evidentes, não se limitando às hipóteses elencadas pelo artigo 5º, II, da LGPD, que o acórdão entendeu como taxativas.

Nesse sentido, Daniel Solove[271], professor na George Washington University Law School, faz críticas às leis de proteção de dados que estabelecem dois níveis de proteção, um para dados comuns e outro para dados sensíveis, já que, para o autor, essa separação não faria sentido no contexto de *Big Data Analytics*, em que grandes quantidades de dados são analisadas rapidamente para extrair outras informações, inclusive através de algoritmos extremamente especializados.

Acrescentando Marcon[272] que dados comuns para a LGPD podem apresentar certa sensibilidade no caso concreto, depende do contexto de inserção do titular[273]. A compra virtual de medicamentos ou a análise de determinadas pesquisas na internet podem levar o algoritmo a gerar um dado sensível de saúde do indivíduo, o qual, se vazado, pode acarretar danos gravosos.

Diante do exposto, vislumbra-se que o entendimento da Corte em questão fora proferido em um cenário de extrema controvérsia sobre o tema. Esta que já poderia ser vislumbrada nas decisões de alguns tribunais, os quais sustentavam que mesmo não havendo o acesso a dados relevantes como cartão de crédito ou senhas, o dano restava comprovado pela violação ocorrida. Inclusive, ante a insegurança causada à vítima por não conseguir mensurar o tamanho do prejuízo material e moral que a situação poderia ocasionar.

Exemplo evidencia-se com a tese exarada pelo Tribunal de Justiça de Minas Gerais[274] na apelação 10000190612994001. O qual sustentou que as consequências que

---

[271] SOLOVE, Daniel. Data is what data does: regulating use, harm, and risk instead of sensitive data. **Northwestern University Law** *Review*, v. 118, jan. 2023, p. 35-36. Disponível em: https://ssrn.com/abstract=4322198. Acesso em: 11 nov. 2023.

[272] MARCON, Daniele Vidal. Dano moral e vazamento de dados: o STJ escreveu certo por linhas tortas? **Consultor Jurídico**, abr. 2023. Disponível em: https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados/. Acesso em: 24 nov. 2023.

[273] “Para vítimas de perseguição e violência doméstica, juízes e médicos que realizam abortos, por exemplo, o endereço onde residem ou a escola onde seus filhos estudam podem ser informações sensíveis. Por outro lado, a orientação sexual e a religião de políticos são dados sensíveis que podem se tornar públicos para fins de identificação das pautas que tais políticos defendem, mas o acesso a sua geolocalização, um dado "comum" para a LGPD, pode causar um assassinato”.

[274] EMENTA: APELAÇÃO CÍVEL - AÇÃO DE INDENIZAÇÃO - VIOLAÇÃO DE SIGILO DE DADOS POR ATAQUE CIBERNÉTICO - DANO MORAL CONFIGURADO - REDUZIR VALOR DA INDENIZAÇÃO. - As consequências que decorreram da invasão dos dados cadastrais da autora por terceiros desautorizados,

decorreram da invasão dos dados cadastrais do titular por terceiros desautorizados, causariam abalos morais, passíveis de indenização. Posto que, o suporte normativo que respalda a reparação do dano moral vincula-se a uma compensação em virtude de lesão a direitos personalíssimos da vítima, nos termos do disposto nos artigos 186 e 927 do Código Civil.

Outrossim, a 30ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo[275] alertou quanto a possibilidade de configuração da quebra no dever de segurança, nos termos do artigo 14 do CDC. Dispondo, mais, que não poderia ser admitida a excludente prevista no § 3º, do artigo 14, do CDC, sob o argumento genérico de que seria uma obrigação da ré manter os seus sistemas atualizados e seguros, evitando que terceiros invadissem e tivessem acesso às informações pessoais de seus consumidores.

Isso posto, o julgado em questão argumentou que não pode ser tratado como mero aborrecimento, o fato de o autor ter dados pessoais em mãos de terceiros não autorizados. Delineando quanto a relevância do número de CPF, endereço, números de telefone fixo e móvel, haja vista que tais são suficientes para abertura de contas, créditos e outros tipos de fraude.

Desse modo, sustentou-se que a protetiva inerente à inviolabilidade dos dados pessoais independeria do uso deles por terceiros, bastando o acesso não autorizado ou a divulgação indevida para configurar ofensa à dignidade da pessoa humana. Assim, o dano moral não precisaria representar a extensão ou o preço associado a uma dor, mas “uma compensação pela ofensa injustamente causada a *outrem*”.

Contudo, a perspectiva adotada pelo STJ é de que dados pessoais comuns, os quais são fornecidos em qualquer tipo de cadastro, não são "acobertados por sigilo, e o conhecimento por terceiro em nada violaria o direito de personalidade", sendo necessário, nesses casos, provar um dano pela sua exposição.

---

causaram abalos moral, passíveis de reparação - Em acordo com as peculiaridades do caso, entendo que o valor da indenização fixada pelo juiz sentenciante deve ser reduzido, O que proporciona a reparação pecuniária do dano à ofendida e o efeito pedagógico ao ofensor, evitando-se a reiteração de condutas dessa natureza, sem que haja enriquecimento ilícito sem causa (TJ-MG - AC: 10000190612994001 MG, Relator: Shirley Fenzi Bertão, Data de Julgamento: 14/08/2019, Data de Publicação: 19/08/2019).

[275] DANO MORAL – VAZAMENTO DE DADOS – CÓDIGO DE DEFESA DO CONSUMIDOR – DEVER DE SEGURANÇA. 1 – Reconhecida a falha no sistema, ante a invasão por terceiros, ocasionando o vazamento de dados pessoais do consumidor, patente o dever de indenizar pelos danos morais sofridos; 2 – Indenização por danos morais fixada no montante pleiteado, ou seja, em R$ 10.000,00, corrigidos do arbitramento e acrescido de juros de mora de 1% ao mês, a partir da citação. RECURSO PROVIDO (TJ-SP - AC: 10001447120218260405 SP 1000144-71.2021.8.26.0405, Relator: Maria Lúcia Pizzotti, Data de Julgamento: 25/08/2021, 30ª Câmara de Direito Privado, Data de Publicação: 13/09/2021).

Nesse diapasão, é notório que o debate em comento se centra nos danos associados ao acesso indevido aos dados pessoais comuns, especialmente considerando a sua capacidade ou não de violar um direito da personalidade. Entretanto, ao direcionar a análise para o acesso indevido a dados sensíveis, em especial os de saúde, torna-se evidente a distinção quanto a possibilidade de violação de questões intimamente vinculadas a aspectos relevantes da personalidade do titular dos dados.

O GDPR prevê, no seu art. 51[276], que as informações pessoais que são, pela sua natureza, particularmente sensíveis em relação aos direitos e liberdades fundamentais "merecem proteção específica, uma vez que o contexto do seu tratamento pode criar riscos significativos para os direitos e liberdades fundamentais".

Isso posto, fica evidente a gravidade exacerbada do acesso indevido a dados sensíveis do paciente, demandando uma tutela ainda mais contundente à segurança dessas informações. O que não invalida determinados aspectos das arguições propostas pelos autores supra, especialmente no que concerne à rápida projeção de um dado sensível através de uma conjunção de dados tidos como comuns, mas que depende da análise casuística da situação concreta.

Contudo, dados com uma linha de confidencialidade mais acentuada, os quais, independente de conversão, podem gerar qualquer tipo de risco à esfera mais sensível da privacidade do indivíduo, devem possuir uma tutela diferenciada.

A salvaguarda da privacidade em questão está intimamente vinculada a efetivação do princípio constitucional da dignidade da pessoa, bem como ao respeito à liberdade das escolhas pessoais de caráter existencial[277]. A ideia de manter o controle sobre as próprias informações mostra-se intrinsecamente ligada a estruturas basilares da própria condição humana de ser para si e ser perante os outros.

Rabindranath[278], em sua obra o Direito Geral de Personalidade, dispõe que o bem da identidade reside na própria ligação de correspondência do homem consigo mesmo e,

---

[276] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados **(Regulamento Geral sobre a Proteção de Dados).** Jornal Oficial da União Europeia. L 119/1, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 29 maio 2024.

[277] LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003. p. 09.

[278] CAPELO DE SOUSA, Rabindranath Valentino Aleixo. **O direito geral de personalidade**. Coimbra: Coimbra Editora, 2011, p. 245.

portanto, atrela-se às profundas necessidades humanas, de modo que o teor da convivência humana acaba dependendo de sua salvaguarda em termos de reciprocidade.

Nesse sentido, Bioni[279] completa delimitando que as informações que influem na projeção de uma pessoa e na sua esfera relacional adéquam-se conceitualmente como um novo direito da personalidade. Desse modo, vislumbra-se a necessidade de tutelada destes.

Para autores como Rodotà[280], a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas. Assim, determinados dados acabam sendo selecionados para terem um caráter de confidencialidade ainda mais acentuado. O que ocorre, por exemplo, com os dados de saúde, o qual guarda em seu bojo um conteúdo altamente passível de discriminação.

Retomando as disposições inerentes à decisão da 2ª Turma do Superior Tribunal de Justiça, em 7 de março de 2023, a qual entendeu que o vazamento de dados pessoais comuns não gera dano moral presumido (*in re ipsa*), houve uma clara distinção com relação ao tratamento dado aos dados de natureza sensível.

Em linhas suscintas, para um adequado aprofundamento na questão, cabe analisar que o dano moral ocorre quando há a demonstração quanto a ocorrência de violação a interesses extrapatrimoniais. A exemplo da integridade psicológica, paz, tranquilidade e, também, dos direitos da personalidade, como nome, intimidade, vida privada e honra. Ressaltando-se, mais, que a noção de dano moral *in re ipsa* elucida a existência de um dano presumido, ou seja, a mera ocorrência do fato já caracteriza o dano. Independentemente de qualquer lastro probatório.

No ordenamento jurídico brasileiro, o autor da ação de indenização deve, pois, provar o prejuízo sofrido. Diferente é o caso do dano moral *in re ipsa*, já que o fato que gerou a lesão já é o suficiente para a comprovação do dano. Este que está presente na própria violação, assim, bastando que o autor prove que houve a prática do ato ilícito.

O dano extrapatrimonial, contudo, por se tratar de afetação anímica, passa a ser configurado, essencialmente, como um dano jurídico, uma vez que suas consequências, como a dor, as frustrações e os sentimentos, ou afetação de bens ou interesses coletivos

---

[279] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019. p. 85.
[280] RODOTÀ, Stefano. **A vida na Sociedade de Vigilância**: privacidade hoje, Rio de Janeiro: Renovar, 2008. p. 56.

decorrem da violação de um direito da vítima. Assim, não precisam representar uma exata medida ou preço da dor, mas uma compensação pela ofensa injustamente causada a outrem.

Nesse interim, tomando por base as protetivas inerentes à personalidade humana, não restam dúvidas quanto a configuração de um dano pelo simples acesso não autorizado aos dados sensíveis dos pacientes, independente de quaisquer provas adicionais. Contudo, o dano sob análise não pode ser reduzido à grave violação à privacidade, atingindo também questões inerentes à estigmatização do indivíduo, a qual pode culminar em sérias questões discriminatórias.

4.1.3 O dano para além da noção de privacidade

Ao versar sobre o dano por acesso indevido a dados sensíveis, muito se discutiu sobre as questões inerentes à violação da privacidade, mas o dano não se limita a esta esfera. Para uma melhor compreensão da presente discussão, mostra-se como necessária a realização da distinção entre o direito fundamental à proteção de dados pessoais e o direito à privacidade. Os quais, apesar de intimamente correlacionados, não possuem a mesma identidade.

Essa distinção é tratada por Bioni[281] sob uma relevante perspectiva, segundo a qual o direito à proteção de dados pessoais angaria autonomia própria. Sendo, pois, um novo direito da personalidade que não estaria atrelado a uma categoria específica. A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade.

Para Rodotà, o primeiro apresenta um âmbito de atuação mais amplo, estabelecendo uma proteção mais extensa. Ao passo que o segundo indica uma visão mais negativa e estática, em larga medida pautada na concepção de impossibilitar a interferência de terceiros[282]. Para o autor, o bem jurídico tutelado na privacidade giraria em torno da informação e do sigilo, ao passo que o direito à proteção de dados abarcaria a informação, a circulação e o seu respectivo controle.

---

[281] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2019. p. 94

[282] RODOTÀ, Stefano. **A vida na Sociedade de Vigilância**: privacidade hoje, Rio de Janeiro: Renovar, 2008. p. 17 e 36.

A compreensão de que estamos tratando sobre categorias distintas parece ser a visão mais acertada sobre o tema. Outrossim, existem uma série de liberdades individuais, vinculadas ao direito à proteção dos dados pessoais, os quais não são abraçadas pelo direito à privacidade. Ressaltando, mais, nas palavras de Bioni, que o centro gravitacional da proteção dos dados pessoais é diferente do direito à privacidade[283].

Passadas as distinções supramencionadas, iniciam-se discussões quanto autodeterminação informativa e o justo receio de estigmatização. Nesse ínterim, para além das questões práticas outrora mencionadas, outros problemas de ordem grave surgem com o vazamento de determinadas informações sensíveis.

Exemplo evidencia-se com a própria questão da estigmatização outrora mencionada. Para Erving Goffman[284], a sociedade estabelece os meios para caracterizar as pessoas, as dividindo em grupos vinculados aos atributos naturalmente perceptíveis[285]. Nesse cenário, o conceito de estigma ganha significado relacional na obra do sociólogo canadense, posto que conecta atributos e estereótipos a formas de estigmatização. Assim, o autor analisa como eles são criados e manipulados, e quais os seus efeitos nas interações sociais.

Retomando algumas discussões outrora efetivadas, cabe relembrar a conceituação do termo "estigma". Este proveniente do grego antigo "*stígmata*", o qual fazia referência a uma marca ou cicatriz feita no corpo, passou, no contexto sociológico e psicológico contemporâneo, a referir-se a uma marca, característica ou reputação que causa uma visão negativa a determinada pessoa ou grupo. Refere-se, pois, a preconceitos, desaprovações ou discriminações embasadas em características, comportamentos ou identidades que são tidas por indesejáveis.

Para uma adequada análise quanto ao dano causado por um processo de estigmatização, cabe remontar alguns dos mecanismos da sua ocorrência. Exemplos evidenciam-se com o fenômeno da criação de estereótipos, preconceitos e discriminações, os quais levam em consideração características dos indivíduos para o estabelecimento de categorizações e padrões de condutas desiguais.

---

[283] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2019. p. 94

[284] GOFFMAN, Erving. **Estigma: la identidade deteriorada**. 5.ed. Buenos Aires: Amorrortu Editores, 1993. p. 11.

[285] “la sociedade estabelece los médios para caracterizar a las personas y el complemento de atributos, que se perciben como corrientes y naturales a los membros de cada uma de essas categorias” (Goffman, 1993, p. 11).

O estabelecimento de estereótipos[286] está, usualmente, vinculado ao enquadramento das pessoas em categorias por meio de etiquetas facilmente reconhecíveis. Atuando, pois, como um atalho mental, simplificado e generalizado, que estabelece contornos quanto à percepção do mundo e dos grupos sociais que nele existem.

Uma das questões mais perigosas do estabelecimento de rótulos vincula-se ao fato de estarem constantemente atrelados a fatores negativos. Os quais acabam sendo reproduzidos culturalmente e interferem nas relações sociais. Goffman[287], inclusive, aponta para a produção de crenças sobre um grupo de pessoas que apresentem características comuns ou pertencentes ao mesmo grupo.

Dispondo, mais, quanto aos riscos inerentes ao rigor no estabelecimento de tais estereótipos, os quais, desacompanhados de uma análise crítica, podem culminar na estruturação de uma base sólida para a formação de preconceitos. Estes que atuam, indevidamente, para fundamentar discriminações e, consequentemente, um tratamento inadequado e desigual em relação a grupos genéricos de pessoas como os imigrantes ou os pertencentes a determinada religião, dentre outros.

A discriminação em questão corrobora com o afastamento desse indivíduo de atividades e oportunidades[288]. Um exemplo claro da vertente conjuntura pode ser observado no acordão do Tribunal Regional do Trabalho da 4ª Região no recurso ordinário 0020175-92.2021.5.04.0373[289]. Neste, fora constatada a ocorrência de uma dispensa discriminatória, constituindo ato atentatório à dignidade da pessoa humana e aos valores sociais do trabalho.

No julgamento proferido em 22/04/2024 pela 3ª Turma, também, ficou comprovada a ocorrência de um “sofrimento e angústia causados ao trabalhador, em razão da discriminação sofrida, bem como porque teve sua fonte de subsistência subtraída, em evidente prejuízo ao reclamante”. Concluiu, mais, que o desligamento do reclamante

---

[286] GOFFMAN, Erving. **Estigma: la identidade deteriorada**. 5.ed. Buenos Aires: Amorrortu Editores, 1993. p. 20.
[287] *Ibid.,* p. 12.
[288] CRUZ, Natalia. Estigma Social**:** O Que é, Significado e Estigmatização. **Quero Bolsa**, 2022. Disponível em: https://querobolsa.com.br/enem/sociologia/estigma-social. Acesso em: 15 nov. 2023.
[289] EMENTA DESPEDIDA DISCRIMINATÓRIA. INDENIZAÇÃO POR DANO MORAL. O dano moral nesse caso é constatado, uma vez que a dispensa discriminatória se constitui em ato atentatório à dignidade da pessoa humana e aos valores sociais do trabalho. Resta caracterizado o sofrimento e angústia causados ao trabalhador, em razão da discriminação sofrida, bem como porque teve sua fonte de subsistência subtraída, em evidente prejuízo ao reclamante.
TRT-4 - ROT: 0020175-92.2021.5.04.0373, Data de Julgamento: 22/04/2024, 3ª Turma.

ocorreu imediatamente após a ciência da reclamada quanto aos problemas de saúde do autor sendo, portanto, discriminatória, “ante a cediça estigmatização de pessoas com deficiência visual”.

Nesse ponto, para além dos prejuízos materiais, resta clara a existência de danos extrapatrimoniais, ante a ofensa à esfera moral e existencial da pessoa física. Sobre esta questão, cabe ressaltar que o reconhecimento pelos outros é, segundo Taylor[290], uma necessidade humana. Posto que, a pessoa apenas se estrutura através da vida social.

De modo que, um indivíduo ou um grupo de pessoas podem sofrer um verdadeiro dano ou uma “autêntica deformação” caso a sociedade que os rodeia “lhes mostre como reflexo, uma imagem limitada, degradante, depreciada sobre ele”. Especialmente, considerando o que Goffman tratou como uma discrepância[291] entre a identidade virtual e a identidade real de um indivíduo, que caso seja conhecida ou manifesta, “estraga a sua identidade social”.

Inclusive, segundo o autor, ela tem como um dos seus efeitos o afastamento da pessoa da sociedade e de si mesmo. Isso de tal forma que pode acabar tornando o indivíduo em alguém desacreditado “frente a um mundo não receptivo”[292].

Trazendo o ponto em comento para o cerne da presente pesquisa, Caitlin Mulholland[293] traz à baila alguns exemplos dados por Cohen quanto às consequências de um tratamento inadequado de dados sensíveis. Este que pode culminar em discriminação e segregação abusiva no âmbito das relações de consumo.

Segundo a autora[294] os dados dos consumidores podem ser utilizados para muitos fins indesejados. Como, para além da mencionada dispensa discriminatória, podem ocorrer

---

[290] TAYLOR, Charles**. La ética de la autenticidad**. Barcelona: Paidos, 1994. 146p.

[291] GOFFMAN, Erving. **Estigma - notas sobre a manipulação da identidade deteriorada**. Tradução em 2004. Disponível em: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mprj.mp.br/documents/20184/151138/goffman,erving.estigma_notassobreamanipulacaodaidentidadedeteriorada.pdf. Acesso em: 05 abr. 2024.

[292] *Ibid.,* p. 47.

[293] MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *In:* MARTINS, G. M.; ROSENVALD, N. (Org.). **Responsabilidade civil e novas tecnologias**. 1ed. Belo Horizonte: Editora Foco, 2020, v. 1, p. 109-124. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 15 nov 2023. p. 5.

[294] consumer data can be used for many purposes to which consumers might not so blithely agree, employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical “have-nots”; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences;

reajustes dos preços cobrados por prestadores de seguros de saúde que excluem ou prejudicam os titulares dos dados a depender da informação sensível de saúde que tiverem acesso.[295]

Ademais, a autora aponta para a existência de uma discriminação, inclusive, no setor de concessão de créditos. Exemplo evidencia-se com o resultado da pesquisa feita por Amitai Etzioni[296] e publicada no *Journal of Law, Medicine & Ethics*, a qual fora objeto de pesquisa do Instituto de Tecnologia e Sociedade[297].

No caso em questão, fora retratada uma grave conjuntura segundo a qual alguns bancos, ao descobrirem que determinados devedores tiveram um derrame, passavam a exigir o pagamento dos empréstimos realizados. “Há pouca ou nenhuma contribuição para o bem comum nessas intervenções, mas sim uma alta intromissão, uma das mais altas que se pode imaginar”.

Para além da estruturação de outros processos discriminatórios atuantes sobre os mais variados vieses, como a deliberação de questões empregatícias e habitacionais baseadas em traços de personalidade percebidos ou em preferências sexuais ou religiosas[298].

---

[295] COHEN, Julie. Examined Lives, Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, p. 1373-1438, 2000. p. 27.

[296] ETZIONI, Amitai. A Communitarian Approach: A Viewpoint on the Study of the Legal and Ethical Policy Considerations Raised by DNA Tests and Databases. **Journal of Law, Medicine & Ethics**, v. 34, p. 217, 2006.

[297] INSTITUTO DE TECNOLOGIA E SOCIEDADE. **Transparência e Governança nos algoritmos, um estudo de caso sobre o setor de birôs de crédito**. Disponível em: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://d26k070p771odc.cloudfront.net/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf. Acesso em: 5 abr. 2024.

[298] DANOS MORAIS. INTOLERÂNCIA RELIGIOSA. AMBIENTE DE TRABALHO DIGNO. RESPONSABILIDADE DO EMPREGADOR. INDENIZAÇÃO DEVIDA. O direito à liberdade de crença, religião e de expressão decorre da proteção constitucional à dignidade da pessoa humana (art. 1º, III, CF). Nessa linha, a Constituição assegura também a liberdade de consciência e livre exercício de cultos religiosos (art. 5º, inciso IV, da CF), bem como o exercício do direito à livre expressão religiosa, filosófica ou política (art. 5º, inciso VIII, da CF). Os mesmos direitos e garantias encontram-se assegurados na Convenção Americana de Direitos Humanos (Pacto de San Jose de Costa Rica) e na Convenção 111 da OIT, ambas ratificadas pelo Brasil. É obrigação do empregador propiciar e zelar por um meio ambiente de trabalho sem práticas discriminatórias, o que inclui a liberdade de crença e religião, sendo sua obrigação adotar providências que impeçam condutas capazes de afetar esses direitos, além de reprimir e não se omitir diante de eventual ofensa ao trabalhador. Trata-se de garantir a integridade e a proteção integral do empregado no âmbito laboral, o que se afina com qualidade de vida e garantia de um ambiente saudável. Verificada a prática de intolerância religiosa no ambiente de trabalho cabe ao empregador, que não adotou medidas preventivas ou saneadoras eficientes indenizar o empregado pelos danos morais decorrentes. Recurso da autora a que se dá provimento para deferir indenização por danos morais (TRT-9 - ROT: 00003703020215090660, Relator: MARLENE TERESINHA FUVERKI SUGUIMATSU, Data de Julgamento: 15/02/2023, 4ª Turma, Data de Publicação: 08/03/2023).

Conforme sugere Bioni[299], uma tutela jurídica dos dados sensíveis busca assegurar que o titular das informações possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto, efetivando a salvaguarda de um traço marcante dos direitos da personalidade.

Estando, em consonância com o outrora disposto, a proteção de dados pessoais intimamente vinculada com a própria liberdade, pincipalmente no que concerne ao processo de autodeterminação informativa. Ora, tal disposição justifica-se com a percepção de que tais dados projetam a maneira como cada indivíduo é visto na sociedade, o que interfere no próprio exercício de direitos e da cidadania.

Passadas as discussões quanto aos possíveis danos por acessos indevidos a dados sensíveis, cabe uma análise quanto a quem deve demonstrar a sua ocorrência. Considerando, para tanto, não apenas questões legais e doutrinárias, mas também aspectos jurisprudenciais.

4.1.4 O ônus da prova nos casos de acesso indevido a dados sensíveis de saúde

Quanto ao ônus probatório[300], nos termos do código de processo civil, tido como a responsabilidade que a parte tem de demonstrar que as suas afirmações e pedidos são verdadeiros, usualmente compete ao autor, no que concerne aos fatos constitutivos de seu direito, e ao réu os fatos impeditivos, modificativos ou extintivos dos direitos da contraparte.

Entretanto, esse alinhamento probatório, por vezes, poderia ocasionar distorções graves, especialmente quando a parte que aciona o juízo não dispuser dos meios adequados de prova. Surge, nesse pronto, a ideia de distribuição dinâmica do ônus da prova, conhecida como Teoria das cargas probatórias dinâmicas.

Para a vertente tese, o ônus probatório deve recair sobre a parte que dispuser de melhores condições para produzi-la. Isso, em conformidade com os princípios processuais da cooperação e da boa-fé. Garantindo uma melhor tutela processual dos interesses dos litigantes.

---

[299] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019, p. 70.

[300] BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Diário Oficial da União, Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 29 maio 2024.

Nesse ponto, o art. 373, § 1º, do CPC dispõe que diante de peculiaridades da causa e em conformidade com as normas legalmente previstas, seria possível a inversão do ônus probatório. Tendo em vista à impossibilidade ou à excessiva dificuldade de cumprir o encargo probatório. Sendo, essa possibilidade de distribuição diversa do ônus em questão atribuída de forma fundamentada pelo juiz.

Trazendo a vertente temática para os contornos do sistema de proteção de dados, cabe colacionar o art. 42, § 2º, da Lei Geral de Proteção de Dados Pessoais (LGPD), o qual previu essa possibilidade, de inverter o ônus da prova em favor do titular de dados pessoais. Assim como ocorre no âmbito do direito do consumidor, que embasa aspectos relevantes da vertente pesquisa.

Conforme expressa previsão no Art. 6º, inciso VIII, do CDC vislumbram-se como direitos do consumidor “a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova”. Esse direito processual é assegurado se houver verossimilhança da alegação, hipossuficiência do consumidor ou titular de dados e demasiado ônus na produção da prova.

Contudo, a despeito do outrora analisado, cabe colacionar uma jurisprudência do Tribunal de justiça do Paraná[301], TJ-PR, que estabelece algumas questões as quais precisam ser observadas. Especialmente, trazendo para a análise da violação dos dados em meio digital.

Na ação que originou a supramencionada decisão, o tribunal entende que não assiste razão à apelante, posto que fora constada a existência de uma mera suposição quanto a ocorrência de um ataque de hackers, não restou clara, sequer, a passagem dos dados do autor da ação pela rede da empresa.

Assim, 4ª Câmara Cível do TJ-PR entendeu pela inexistência de fundados indícios da ocorrência do ilícito, evidenciando que se tratam de apenas suposições levantadas pela apelante como justificativa para o prejuízo financeiro sofrido. Portanto, não caberia a

[301] APELAÇÃO CÍVEL – AÇÃO CAUTELAR DE PRODUÇÃO ANTECIPADA DE PROVAS – SENTENÇA DE EXTINÇÃO, SEM JULGAMENTO DE MÉRITO – ALEGAÇÃO DE POSSIBILIDADE DA QUEBRA DO SIGILO DE DADOS TELEMÁTICOS EM PRODUÇÃO DE PROVA ANTECIPADA – AUSÊNCIA DE FUNDADOS INDÍCIOS DA OCORRÊNCIA DO ILÍCITO ALEGADO – PRESSUPOSTO LEGAL PREVISTO NO ART. 22, PARÁGRAFO ÚNICO, INCISO I, DA LEI Nº 12.965/2014 – SENTENÇA MANTIDA – RECURSO CONHECIDO E DESPROVIDO. Apelante que não comprovou a existência de fundados indícios de ataque de “hackers” na sua rede de internet. (TJPR - 4ª C.Cível - 0065236-35.2020.8.16.0014 - Londrina - Rel.: DESEMBARGADORA REGINA HELENA AFONSO DE OLIVEIRA PORTES - J. 04.05.2021).

concessão do acesso aos dados quanto a registros de conexão ou de acesso a aplicações de internet, nos termos do artigo 22 da lei n.º 12.965/2014.

O dispositivo normativo citado assegura o fornecimento dos registros em questão para auxiliar a parte na formação de um conjunto probatório em processo judicial, quer seja incidental ou autônomo, cível ou penal. Contudo, para que o juiz ordene o fornecimento dos dados requisitados ao responsável pela sua guarda é necessário que o requerimento do interessado contenha algumas formalidades[302], as quais devem estar presentes sob pena de inadmissibilidade da solicitação.

Dentre as quais, cabe mencionar a necessária existência de fundados indícios da ocorrência do ilícito, bem como deve constar uma justificativa adequadamente motivada quanto a utilidade dos registros solicitados, especialmente, para fins de investigação ou instrução probatória. Devendo, mais, ser estabelecido o período ao qual se referem os registros requisitados.

Para uma melhor compreensão quanto a necessidade de atender as requisições normativas para o fornecimento destes registros, cabe distingui-los[303], posto que tais logs, como são conhecidos, quer sejam de conexão ou de acesso, representam peças-chave no funcionamento seguro e adequado da internet.

Inicialmente, os registros de conexão vinculam-se às informações técnicas relacionadas à conexão do usuário à internet. De modo que, acabam abarcando fatores como o endereço IP, tipo de dispositivo utilizado, horários de conexão, a localização do usuário, entre outros. Tais informações estão diretamente vinculados à busca pela segurança das comunicações online.

Estes que, inclusive, auxiliam “na identificação de possíveis ameaças, a investigação de atividades suspeitas e a manutenção da integridade da rede”. Garantindo um adequado controle quanto à gestão do sistema.

Ao passo que os registros de acesso a aplicações na internet estão atrelados às informações sobre a atividade de um usuário na rede. Consideram, pois, questões

---

[302] BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 maio 2024.

[303] ANDRADE, Walmar Andrade. **A guarda de registros de conexão e de acesso a aplicações, conforme o Marco Civil da Internet**. Disponível em: https://walmarandrade.com.br/guarda-de registros/#:~:text=Os%20registros%20de%20conex%C3%A3o%20e,conex%C3%A3o%20do%20usu%C3%A1rio%20%C3%A0%20internet. Acesso em: 22 mar. 2024.

correlacionadas aos sites visitados, aos aplicativos utilizados e às ações realizadas durante a navegação. Estando, pois, associados ao comportamento dos usuários e à identificação de padrões de uso.

Portanto, fica evidente a possibilidade de propositura de ação para que se forme conjunto probatório, porém os requisitos legais outrora analisados devem ser preenchidos para que a produção antecipada de provas, referente aos dados protegidos pela mencionada lei, seja deferida.

Tal regramento vincula-se à “relevante proteção constitucional e infralegal conferida aos dados a que se pretende ter acesso, como meio de se evitar o uso indevido desses dados e possíveis violações a direitos como privacidade e intimidade dos usuários”.

Traçado o panorama supramencionado, cabe analisar alguns aspectos práticos quanto às consequências do acesso indevido a dados sensíveis na esfera indenizatória.

4.2 CONSEQUÊNCIAS DO ACESSO INDEVIDO AOS DADOS SENSÍVEIS DOS PACIENTES E A ESFERA INDENIZATÓRIA

4.2.1 As facetas do dano patrimonial no incidente de segurança

Em linhas iniciais, os danos patrimoniais se caracterizam por um prejuízo econômico, proveniente de uma diminuição imediata do patrimônio da vítima ou o impedimento de obtenção de vantagem futura que razoavelmente poderia esperar obter, caso não houvesse a conduta antijurídica do agente[304].

Essa modalidade de dano demanda a existência de provas concretas dos prejuízos efetiva e potencialmente sofridos, não podendo ser presumidos. Desse modo, cabe ao titular dos dados o dever de fazer prova concreta do dano para que o hospital seja responsabilizado.

Para o avançar das discussões neste tema, cabe retomar o recorte outrora realizado quanto a aplicação da responsabilidade objetiva ao caso, a qual possibilita a reparação de um dano cometido sem culpa, se satisfazendo apenas com o dano e o nexo de causalidade.

---

[304] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 jan. 2024.

Nesse cenário, fala-se em culpa prescindível, posto que a responsabilidade se funda em outros parâmetros já exaustivamente delineados.

Cabe reiterar quanto a indispensável demonstração da existência do vínculo de causalidade entre a ação e o dano. Posto que, conforme discussões já travadas, com a exclusão da culpa como requisito da responsabilização, ganha contornos significativos a relação lógica de causalidade entre uma conduta e a consequência danosa sobre o qual se deseja imputar o dever de indenizar.

Quanto ao dano, este se divide em patrimonial e extrapatrimonial, ou seja, respectivamente com e sem repercussão na órbita financeira do ofendido. Sobre esse elemento, cabe mencionar que a doutrina majoritária se finca no pressuposto de que sem a prova do dano, ninguém poderia ser civilmente responsabilizado. Comprovação esta que pode estar atrelada à dimensão do dano, como nos casos de prejuízos materiais, ou na ocorrência de lesão a bem ou interesse juridicamente tutelado, como ocorre com os prejuízos materiais.

Passadas tais colocações introdutórias, cabe tecer algumas considerações quanto a ocorrência do dano patrimonial no incidente de segurança. Incialmente, uma primeira faceta ganha contornos evidentes, qual seja a concretização de fraudes por conta da informação confidencial disponibilizada, a qual ocasiona a formação de uma conjuntura extremamente gravosa para a esfera patrimonial e moral do indivíduo.

Os mecanismos de atuação fraudulenta apresentam variadas manifestações. Como os registros dos pacientes têm quase tudo que um invasor precisa em um único documento, assim, tem-se a possibilidade de realização de esquemas sofisticados de fraude em seguros, roubo total de identidade do titular dos dados ou mesmo a venda ilegal dessas informações no mercado ilegal. Já que uma vez expostos, os dados podem ser leiloados na *dark web*.

A disponibilização irregular com fito lucrativo alcança, também, o roubo propriedade intelectual[305], dados de pesquisa, informações quanto a testes de medicamentos, registros médicos e similares. Tais dados de investigação roubados, muitas vezes representam um investimento financeiro significativo, o qual vincula-se a anos de investigação e ensaios

[305] FUENTES, Maricel Rivera; HUQ, Nashid. **Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks**. Disponível em: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf. Acesso em: 26 abr. 2024.

dispendiosos em pacientes. Trazendo mais uma relevante preocupação quanto a salvaguarda adequada dos sistemas de armazenamento de dados.

Cabe mencionar que boa parte dos criminosos cibernéticos se especializam em encontrar instâncias de nuvem inseguras e bancos de dados vulneráveis[306]. Estes que contêm números de cartão de crédito, números de previdência social e outras informações de identificação pessoal ou de cunho sensível.

Os quais podem ser usados para fraude bancária ou aplicação de spam[307]. Esse grave contexto pode ser de tão simples acesso quanto usar consultas de pesquisa no Google. O que amplia a possibilidade de concretização de danos materiais significativos.

Outrossim, uma outra forma de ocasionar prejuízo material por meio do acesso indevido a dados, especialmente os de cunho sensível, é a extorsão. Esta ocorre quando as informações são mantidas indevidamente sob a posse dos cibercriminosos em troca de resgate financeiro ou para causar danos à reputação em caso de não fornecimento do valor requerido pelos infratores.

Nessa modalidade, as ocorrências mais frequentes estão vinculadas ao uso dos outrora mencionados *ransomware*, um tipo de malware que sequestra os dados de uma organização, podendo paralisar as operações de uma empresa, interrompendo o acesso a sistemas críticos e aplicativos.

Além disso, os dados, por exemplo dos prontuários, são sequestrados, podendo ocasionar perda do histórico dos pacientes ou demais informações importantes e confidenciais, incluindo dados de clientes, informações financeiras e dados de propriedade intelectual, está presente, em especial, nos hospitais universitários.

Esse fenômeno, para além dos danos extrapatrimoniais presentes, pode acarretar um prejuízo financeiro significativo voltado aos custos de reposição de dados relevantes, em especial dos pacientes em atendimento, os quais precisam do histórico devidamente atualizado para a resolução das questões de saúde que enfrentam.

Considerando, mais, os danos inerentes ao não funcionamento de alguns serviços em casos de ataques cibernéticos. Como o caso dos hospitais administrados pela empresa

---

[306] TUNGGAL. Allan Toh. What is a Data Leak? Stop Giving Cybercriminals Free Access. **UpGuard,** 2023. Disponível em: https://www.upguard.com/blog/data-leak. Acesso em: 26 dez. 2023.

[307] Com tantas informações de cunho pessoal, a realização de golpes por e-mail encontra-se amplamente facilitada. Especialmente, quando o agente mal-intencionado, sabendo a instituição bancária utilizada pelo indivíduo e os dados a ela atrelados, elabora e-mails se passando pela instituição financeira. Conquistando, mais facilmente, a confiança do usuário.

Prospect Medical Holdings[308], os quais ficaram com suas atividades paralisadas em vários estados dos Estados Unidos em decorrência de um ataque cibernético, o que se mostra ainda mais grave.

Para além dessas situações, existe a própria dinâmica de extorsão individualizada, na qual cibercriminosos ameaçam divulgar os dados dos pacientes em caso de não prestarem uma contraprestação financeira. Assim, os custos ultrapassam o pagamento do resgate exigido pelo cibercriminoso, incluindo despesas adicionais relacionados à recuperação de dados e dispêndios com consultorias e orientações jurídicas ou em outras áreas correlatas.

Entretanto, apesar de a conjuntura ser extremamente inoportuna, a jurisprudência pátria analisará adequadamente o caso concreto para configuração ou não do dever de indenizar, mesmo diante da ocorrência de uma fraude. Nesse cenário, surgiram duas correntes jurisprudenciais distintas em um mesmo período temporal. Segue-se, pois, a análise destas.

Ambas versam sobre alega falha na segurança dos procedimentos do hospital, ante ao vazamento de informações confidenciais do paciente que ali estava internado, possibilitando a ocorrência de um golpe financeiro. No caso, terceiros tiveram acesso a dados confidenciais extraídos do prontuário da paciente, os quais estavam sob a guarda do hospital, circunstância que possibilitou que a filha da paciente fosse vítima de estelionato.

Por um lado, sobre o tema, a 5ª Turma Cível do Tribunal de Justiça do Distrito Federal posicionou-se na apelação cível 0708698-23.2021.8.07.0009[309], entendendo que

---

[308] ASSOCIATED PRESS. Ataque hacker interrompe funcionamento de hospitais nos Estados Unidos e FBI abre investigação. **Globo**, 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/08/10/ataque-hacker-interrompe-funcionamento-de-hospitais-nos-estados-unidos-e-fbi-abre-investigacao.ghtml. Acesso em: 05 jan. 2024.

[309] (...) PRONTUÁRIO DE PACIENTE INTERNADO NO HOSPITAL. INFORMAÇÕES. ACESSO INDEVIDO. FRAUDE. DEVER DE GUARDA. FALHA NA PRESTAÇÃO DO SERVIÇO. DANO MATERIAL E DANO MORAL. CONFIGURAÇÃO. VALOR ARBITRADO. RAZOÁVEL E PROPORCIONAL. (...) Na espécie, é notória a pertinência subjetiva, se a parte autora alega falha na segurança dos procedimentos do hospital réu, que deixou vazar informações confidenciais da paciente (genitora da autora), que ali estava internada, possibilitando o golpe e a consequente reparação pelos danos suportados. 2. A responsabilidade objetiva pelo fato do serviço na relação de consumo, consoante o art. 14 do CDC, é oponível aos hospitais na parcela dos serviços relacionados ao estabelecimento empresarial, a exemplo da internação, alimentação, instalações e serviços auxiliares. No caso, presente a falha na prestação de seu serviço, porquanto terceiros tiveram acesso a dados confidenciais extraídos do prontuário da paciente que estavam sob a guarda do hospital, circunstância que possibilitou que a autora (filha da paciente) fosse vítima de estelionato. 3. Diante de evidente negligência do hospital na guarda das informações pessoais da paciente, possibilitando a manobra fraudulenta, impõe-se o ressarcimento da quantia desembolsada pela vítima da fraude. 4. Atingido o direito da personalidade diretamente, o dano moral (puro ou direto) estará vinculado à própria existência do fato (*in*

houve evidente negligência do hospital na guarda das informações pessoais da paciente, restando possibilitada a manobra fraudulenta. Portanto, o Tribunal concluiu pela imposição do ressarcimento da quantia desembolsada pela vítima da fraude, considerando, mais, a compensação do aspecto moral inerente à questão.

O decisum arguiu, mais, quanto o evidente e "considerável" agravamento do estado de saúde da paciente, titular dos dados vazados e mãe da vítima do golpe financeiro, atingiu a própria personalidade da vítima da fraude, a deixando em situação de fragilidade emocional. Defendendo, por fim, que "sem olvidar as finalidades compensatória, punitiva ao ofensor, pedagógica e preventiva da condenação, bem assim às circunstâncias da causa, inclusive a capacidade das partes, afigura-se adequado o valor fixado na sentença".

Por outro lado, exemplo divergente do outrora apresentado encontra-se no acordão da 36ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo[310], a qual dispôs que a vítima "fora devidamente informada e alertada acerca da modalidade do golpe praticado e dos cuidados que deveriam ser adotados para evita-lo".

---

re ipsa), cujos resultados são presumidos, ao contrário de quando é atingido o direito da personalidade mediante lesão a bens de natureza patrimonial (dano moral impuro ou indireto). 5. Na hipótese, é inegável que o agravamento considerável do estado de saúde da paciente atinge a personalidade jurídica da autora, que se encontrava em situação de fragilidade emocional em virtude da internação de sua genitora. Assim, sem olvidar as finalidades compensatória, punitiva ao ofensor, pedagógica e preventiva da condenação, bem assim às circunstâncias da causa, inclusive a capacidade das partes, afigura-se adequado o valor fixado na sentença. 6. Apelações conhecidas e não providas. TJDF. 5ª Turma Cível. Processo N. APELAÇÃO CÍVEL 0708698-23.2021.8.07.0009 APELANTE(S) ELISSANDRA DE MELO E SILVA e HOSPITAL SANTA MARTA LTDA APELADO(S) HOSPITAL SANTA MARTA LTDA e ELISSANDRA DE MELO E SILVA Relator Desembargador FÁBIO EDUARDO MARQUES. Acórdão Nº 1616700, DJe em 03/10/2022[309](Grifo meu).

[310] APELAÇÃO. Reparação de danos. Golpe do hospital. Suposta falha na prestação do serviço. Sentença de procedência. Irresignação. Cabimento. Autora, acompanhante do irmão em internação hospitalar, que recebe ligação telefônica de falsário, no quarto de internação. Estelionatário que se identifica como médico responsável pelo tratamento do irmão e negocia a venda de suposto medicamento de alto custo indispensável ao tratamento, mas não incluído na cobertura do plano de saúde/convênio. Golpista, suposta secretária do "médico", que em seguida solicita os dados e a realização de transferência bancária em conta de terceiro para a concretização do negócio. Celebração do contrato de prestação de serviços médico-hospitalares de internação. Ocasião em que a autora fora devidamente informada e alertada acerca da modalidade do golpe praticado e dos cuidados que deveriam ser adotados para evita-lo. Contrato com expressa previsão no sentido de que as despesas não cobertas pelo plano/seguro saúde seriam pagas de forma presencial, mediante a emissão de boleto pelo nosocômio. Higidez contratual sequer discutida. Prova coligida no sentido de que o dano ocorreu por fortuito externo e culpa exclusiva da consumidora, que agiu sem adotar as cautelas necessárias e inerentes à obrigação em testilha. Responsabilidade, ainda que objetiva do hospital-apelante, elidida em face à inexistência do nexo de causalidade. Artigos 186 e 927, ambos do CCB, e artigo 14, § 3º, inciso II, do CDC. Sentença reformada. Recurso provido

[310] SÃO PAULO. Tribunal de Justiça de São Paulo. **AC: 11074313820218260100 SP 1107431-38.2021.8.26.0100**, Relator: Lidia Conceição, Data de Julgamento: 05/10/2022, 36ª Câmara de Direito Privado, Data de Publicação: 05/10/2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1285322229/inteiro-teor-1285322264. Acesso em: 29 maio 2024.

Inclusive, segundo as provas coligadas aos autos, no próprio contrato constava expressa previsão no sentido de que as despesas não cobertas pelo plano de saúde seriam custeadas presencialmente, com a emissão de boleto pelo nosocômio. O que, segundo o Tribunal, sequer discutido.

Assim, concluiu-se que a responsabilidade da instituição hospitalar fora elidida, ante a ausência do nexo causal. Este rompimento na cadeia causal se caracterizou pela materialização do dano através de um "fortuito externo e culpa exclusiva da consumidora, que agiu sem adotar as cautelas necessárias e inerentes à obrigação em testilha".

Nesse sentido entendeu o Superior Tribunal de Justiça no agravo em recurso especial nº 2008070 – SP de relatoria do Ministro Luis Felipe Salomão[311]. Segundo o qual, sustentou-se que apesar da falha do nosocômio quanto à guarda dos dados da paciente, o que efetivamente ensejou o sucesso da fraude fora a manifesta falta de cuidado da vítima, a qual, mesmo em estado de estresse, não lhe eliminava a incumbência de agir com cautela.

Afinal, para caso concreto, apesar da circunstancia envolver internação coberta pelo plano de saúde, "a pedido de um estranho por meio de telefone ao quarto do hospital a autora realizou depósito em conta bancária de desconhecido, sem ao menos consultar acerca do ocorrido o hospital onde se encontrava, medida que só tomou posteriormente". Evidenciando o rompimento do nexo causal. Não cabendo a aplicação de uma responsabilização com intuito punitivo, mas tão somente reparatório.

Uma outra perspectiva está relacionada a perdas financeiras e patrimoniais decorrentes da disponibilização da informação sob a vertente da aplicação de processos discriminatórios, os quais interferem no aspecto patrimonial da dinâmica socio-relacional. A vertente questão demanda um lastro probatório vasto para que seja configurada. O que se distingue da comprovação do dano extrapatrimonial dessa ocorrência.

Nesse ponto, urge recordar o recurso ordinário 0020175-92.2021.5.04.0373, julgado em abril de 2024 pela 3ª Turma do TRT-4. No qual, o Tribunal concluiu pela ocorrência de uma dispensa discriminatória concretizada após a ciência, pela reclamada, dos problemas de saúde do autor e de seu afastamento do serviço.

---

311 BRASIL. Superior Tribunal de Justiça. **AREsp: 2008070 SP 2021/0356249-0**. Rel. Min. Luis Felipe Salomão. DJe 08/02/2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1373329300. Acesso em: 29 maio 2024.

No âmbito patrimonial, com fulcro no art. 4º da Lei 9.029/95 o qual faculta ao empregado optar entre a readmissão com ressarcimento integral de todo o período de afastamento ou a percepção, em dobro, da remuneração do período de afastamento, o decisum determinou a reintegração do reclamante ao emprego.

A faculdade exercida pelo autor culminou, também, no pagamento dos salários do período de afastamento, acrescidos do adicional de insalubridade, devidos desde o primeiro dia subsequente à despedida, deduzidos os valores referentes ao período de aviso prévio indenizado comprovadamente pago. Cabendo, mais, o 13º salário, as férias acrescidas de 1/3 e o FGTS do período de afastamento, deduzido o pagamento efetuado no TRCT a tais títulos e o valor recebido pelo autor a título de indenização compensatória de 40% sobre o FGTS.

De modo que o dano patrimonial sob análise consiste na vantagem econômica a qual o reclamante deveria obter no curso normal de sua atividade, porém restou impossibilitado em razão da conduta antijurídica do agente. Cabendo à vítima fazer prova da ocorrência de tais danos[312]. Sendo o *quantum* devido fixado através da razoabilidade dos ganhos que deixam de ser obtidos pela vítima, sob a ótica de padrões objetivos para sua aferição, e tomando por base a normativa vigente.

Para além do exemplo colacionado, tem-se o dever de reparar danos denominados pela doutrina especializada como emergentes. Estes que, normalmente, corresponderiam ao resultado aritmético entre o antes e o depois do patrimônio da vítima, tomando como referência o acontecimento da lesão.

Contudo, como o fito da reparação vincula-se a restituição do estado anterior à sua ocorrência do dano, nem sempre a indenização será pautada na correspondência entre o valor da perda econômica.

Passadas essas considerações, cabe analisar uma outra perspectiva inerente ao dano por acesso indevido aos dados sensíveis, em especial os de saúde. Trazendo, pois, o presente enfoque para o dano moral.

---

[312] MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 15 fev. 2024.

4.2.2 Aspectos relevantes quanto à fixação indenizatória do dano extrapatrimonial

O dano extrapatrimonial consiste na lesão a interesses e bens jurídicos não patrimoniais, ocasionados pela conduta danosa. Sendo, pois, uma afetação anímica, passando a ser configurado como um dano jurídico. De modo que, suas consequências decorrem da violação de um direito da vítima. O qual fora por muito tempo associado, apenas, às dores, às frustrações e aos sentimentos, mas que ganhou, posteriormente, contornos muito mais atrelados à afetação negativa bens imateriais ou interesses pessoais.

Para uma adequada análise do presente tópico, urge recordar o caso da dispensa discriminatória outrora analisada. No qual, para a configuração do dano extrapatrimonial, ao reclamante bastou a comprovação de que o desligamento das suas atividades estava diretamente associado a uma clara discriminação. Esta evidenciada após a reclamada tomar conhecimento do quadro de saúde do autor da ação.

Assim, o dano moral daí decorrente é presumível, não requerendo quaisquer outras evidencias de dano psíquico ou demais consequências gravosas à sua esfera intrapessoal. O fato, por si, é suficiente para a caracterização do dano em questão, ante a sua capacidade de ocasionar uma violação à dignidade do trabalhador. A qual pode ser evidenciada na estigmatização sofrida pelo reclamante por se encontrar acometido de doença visual, que compromete, inclusive, sua recolocação no mercado de trabalho.

Restando clara a violação aos direitos de personalidade do autor, “posto que ao despedi-lo a ré estava ciente de que apresentava problema de saúde, o que o privou de seu meio de subsistência em momento de acentuação de sua doença”[313].

Desse modo, o caso em questão envolveu uma conduta discriminatória decorrente do acesso a dado sensível do autor da ação que, por sua vez, ocasionou uma grave consequência para o titular do dado. Contudo, especialmente considerando a violação a dado sensível, a existência de uma conjuntura fática gravosa gerada pelo acesso ao dado não é requisito para a configuração do dano sob análise.

---

[313] EMENTA DESPEDIDA DISCRIMINATÓRIA. INDENIZAÇÃO POR DANO MORAL. O dano moral nesse caso é constatado, uma vez que a dispensa discriminatória se constitui em ato atentatório à dignidade da pessoa humana e aos valores sociais do trabalho. Resta caracterizado o sofrimento e angústia causados ao trabalhador, em razão da discriminação sofrida, bem como porque teve sua fonte de subsistência subtraída, em evidente prejuízo ao reclamante. TRT-4 - ROT: 0020175-92.2021.5.04.0373, Data de Julgamento: 22/04/2024, 3ª Turma.

Nesse interim, pode-se afirmar que o simples acesso indevido a dados sensíveis é suficiente para a configuração do dano extrapatrimonial ao titular do dado, independente de quaisquer outras provas adicionais. Configurando, pois, um dano moral presumido. Especialmente tomando por base todas as discussões outrora realizadas quanto a aspectos inerentes à formação da personalidade, à relevância da autodeterminação informativa, à necessária observância da privacidade e ao risco de estigmatização.

Inclusive, cabe retomar a distinção feita pela 2ª Turma do Superior Tribunal de Justiça, em 7 de março de 2023. Segundo a qual entendeu que o vazamento de dados pessoais comuns não gera dano moral presumido, *in re ipsa*, requerendo a comprovação, pelo titular dos dados, de eventual dano decorrente da exposição dessas informações[314], o que é diferente do caso de vazamento referente a dado sensível.

Assim, independente da discordância da doutrina especializada quanto ao dano extrapatrimonial por vazamento de dado pessoal comum, a jurisprudência mais recente filia-se a necessidade da demonstração do dano sofrido. Abrindo, quanto ao dado sensível, expressa divergência tanto por sua natureza, quanto pela necessária salvaguarda das protetivas a ele atreladas.

Passadas essas considerações, traz-se à baila, inicialmente, que a reparabilidade do dano moral encontra tutela constitucional expressa no artigo 5º, incisos V e X, da Constituição Federal. Estes dispositivos orientam não apenas quanto a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, como também ressaltam o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem decorrente de sua violação.

Inclusive, acrescentasse que o dano moral decorrente da mencionada lesão a atributos da personalidade, funda-se em um outro pressuposto constitucional de extrema relevância, qual seja a dignidade da pessoa humana[315], princípio central da Constituição. Assim, resta demonstrada a necessária aplicabilidade desse aparato indenizatório para uma tutela contundente de preceitos caros ao ordenamento jurídico vigente.

---

[314] BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Relator: Min. FranciscoFalcão, 07 mar. 2023. Disponível em:https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28ARESP.clas.+e+%40num%3D%222130619%22%29+ou+%28ARESP+adj+%222130619%22%29.suce.&O=JT. Acesso em: 03 mar 2023.

[315] BRASIL. **Constituição (1988).** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 maio 2024.

Quanto à fixação da indenização por dano moral, Miragem[316] elucida sobre o desafio da definição de critérios para arbitramento dos valores devidos, ante a sua natureza insuscetível de avaliação econômica. Dispondo, mais, quanto a impossibilidade de atribuir antecipadamente valor a danos dessa natureza, “sobretudo quando se tratar de lesões que afetam atributos considerados inestimáveis, como é o caso dos atinentes à personalidade”.

Nesse diapasão, existe um relevante julgado do STF[317], segundo o qual a fixação do valor de indenização por dano moral, na esfera trabalhista, seria constitucional desde que sirva apenas como parâmetro para a fundamentação da decisão judicial. Não sendo, portanto, um elemento limitador do quantum devido. Este que deve ser estabelecido com base nas nuanças do caso concreto[318].

O entendimento em questão fora prolatado em um cenário em que a esfera trabalhista apresentava um tabelamento legalmente estruturado nos arts. 223-A a 223-G da CLT. Os quais foram objeto de uma ação direta de inconstitucionalidade. Contudo, tal julgado pode ser aplicado para outros setores.

Entendimento que reforça a impossibilidade de subtração da prerrogativa do magistrado de realizar o arbitramento do dano extrapatrimonial, especialmente, em decorrência da existência de um tabelamento legalmente estipulado. Entretanto, o vertente decisum não coaduna com a proibição quanto a fixação de métodos que auxiliem o julgador a estabelecer a quantificação do dano extrapatrimonial.

---

316 MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 fev. 2024.

317 É constitucional o tabelamento para fins de fixação do valor de indenização por dano moral trabalhista previsto na Consolidação das Leis do Trabalho (CLT). Contudo, os montantes elencados na lei não podem ser interpretados como um “teto”, mas apenas servem como parâmetro para a fundamentação da decisão judicial, de modo a permitir que ela, desde que devidamente motivada, determine o pagamento de quantias superiores. Com base nesse entendimento, o STF julgou parcialmente procedentes as ADIs para conferir interpretação conforme a Constituição e estabelecer que: (i) as redações conferidas aos art. 223-A e 223-B, ambos da CLT, não excluem o direito à reparação por dano moral indireto ou dano em ricochete (dano reflexo) no âmbito das relações de trabalho, a ser apreciado nos termos da legislação civil; e (ii) os critérios de quantificação de reparação por dano extrapatrimonial previstos no art. 223-G, caput e § 1º, da CLT, deverão ser observados pelo julgador como orientativos de fundamentação da decisão judicial, sendo constitucional, porém, o arbitramento judicial do dano em valores superiores aos limites máximos dispostos nos incisos I a IV do § 1º do art. 223-G, quando consideradas as circunstâncias do caso concreto e os princípios da razoabilidade, da proporcionalidade e da igualdade. STF. Plenário. ADI 6.050/DF, ADI 6.069/DF e ADI 6.082/DF, Rel. Min. Gilmar Mendes, julgados em 26/06/2023 (Info 1100).

318 No âmbito doutrinário, tem-se o Enunciado n. 550VI da Jornada de Direito Civil de 2013. Este que reforçou que a quantificação da reparação por danos extrapatrimoniais não deveria estar atrelada a tabelamento ou ao estabelecimento de valores fixos.

Ora, a ausência de critérios para a quantificação dos danos extrapatrimoniais pode ocasionar significativas preocupações, em especial no âmbito da segurança jurídica. Outrossim, a inexistência de parâmetros objetivamente auferíveis afetaria a previsibilidade quanto à extensão das sanções reparatórias.

Nesse sentido, o STJ passou a adotar "método bifásico"[319], segundo o qual estabelece-se um valor básico para a indenização tomando por base o interesse jurídico lesado e um grupo de precedentes. Passada essa etapa inicial, caberia uma análise das circunstâncias do caso para a fixação, em definitivo, da reparação. Considerando a gravidade do fato, o envolvimento da vítima, a condição econômica das partes, dentre outras questões[320].

A Corte acrescenta que em detrimento "da impossibilidade de uma indenização pecuniária que compense integralmente a ofensa ao bem ou interesse jurídico lesado"[321], caberia a busca por uma reparação satisfatória, pautada pela equidade, apesar de não guardar, por sua natureza, uma relação de equivalência[322] precisa com o prejuízo extrapatrimonial.

---

[319] BRASIL. Supremo Tribunal Federal. **O método bifásico para fixação de indenizações por dano moral.** Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-10-21_06-56_O-metodo-bifasico-para-fixacao-de-indenizacoes-por-dano-moral.aspx. Acesso em: 05 abr 2024.

[320] Na jurisprudência, veja-se, exemplificativamente: STJ, REsp 1.152.541/RS, Rel. Min. Paulo de Tarso Sanseverino, 3ª Turma, j. 13/09/2011, DJe 21/09/2011; STJ, REsp 1669680/RS, Rel. Min. Nancy Andrighi 3ª Turma, j. 20/06/2017, DJe 22/06/2017.

[321] RECURSO ESPECIAL. RESPONSABILIDADE CIVIL. DANO MORAL. INSCRIÇÃO INDEVIDA EM CADASTRO RESTRITIVO DE CRÉDITO. QUANTUM INDENIZATÓRIO. DIVERGÊNCIA JURISPRUDENCIAL. CRITÉRIOS DE ARBITRAMENTO EQUITATIVO PELO JUIZ. MÉTODO BIFÁSICO. VALORIZAÇÃO DO INTERESSE JURÍDICO LESADO E DAS CIRCUNSTÂNCIAS DO CASO. (...)4. Elevação do valor da indenização por dano moral na linha dos precedentes desta Corte, considerando as duas etapas que devem ser percorridas para esse arbitramento.
5. Na primeira etapa, deve-se estabelecer um valor básico para a indenização, considerando o interesse jurídico lesado, com base em grupo de precedentes jurisprudenciais que apreciaram casos semelhantes.
6. Na segunda etapa, devem ser consideradas as circunstâncias do caso, para fixação definitiva do valor da indenização, atendendo a determinação legal de arbitramento equitativo pelo juiz.
7. Aplicação analógica do enunciado normativo do parágrafo único do art. 953 do CC/2002.
8. Arbitramento do valor definitivo da indenização, no caso concreto, no montante aproximado de vinte salários mínimos no dia da sessão de julgamento, com atualização monetária a partir dessa data (Súmula 362/STJ).
STJ - RESP: 1.152.541 - RS, Relator: Ministro Paulo de Tarso Sanseverino, Data de Julgamento: 13/09/2011.

[322] "Para provar o dano moral em sua existência e entidade não é necessário aportar prova direta, senão que o juiz deverá apreciar as circunstâncias do fato, e as qualidades da vítima, para estabelecer objetiva e presuntivamente o agravo moral, na órbita reservada da intimidade do sujeito passivo. Não acreditamos que o agravo moral deve ser objeto de prova direta, pois isso resulta absolutamente impossível pela índole do mesmo que reside no mais íntimo da personalidade, embora se manifeste, às vezes, por sinais exteriores, que podem não ser autêntica expressão. Ninguém pode indagar o espírito de outrem tão profundamente como para poder afirmar com certeza a existência e a intensidade da dor, a verdade de um padecimento, a realidade da angústia ou da decepção" (Jorge Bustamante Alsina, Eqüitativa Valuación Del Daño, p. 655, apud Antonio Jeová Santos,Dano Moral Indenizável, 2a ed., Lejus, 1999, p. 528)

Outrossim, cabe um recorte feito pelo Ministro Sanseverino quanto à dinâmica estabelecida em Portugal, segundo a doutrina de Almeida Costa[323]. Especialmente considerando algumas similitudes com a visão outrora apresentada.

No art. 496, n. 3, do CC português, preceitua-se uma indenização por danos morais pautada segundo critérios de equidade, a qual deve observar questões inerentes à extensão, à gravidade dos danos e a todas as outras circunstâncias que corroborem para uma solução equitativa. Quer estejam vinculadas à situação econômica responsável e do lesado, como, sendo o caso, à culpa do agente.

Sanseverino[324], nesse ponto, evidencia que por tratar-se de um método o qual preceitua a aplicação da razoabilidade e de critérios objetivamente auferíveis, não caberia qualquer sustentação a fundamentar a existência de um poder arbitrário.

Nesse ponto, Miragem[325] elenca alguns dos mencionados critérios a serem utilizados, trazendo mais praticidade para a presente pesquisa. Exemplo evidencia-se com a análise da repercussão do dano na esfera jurídica da vítima.

Por meio da qual observa-se a intensidade do sofrimento experimentado, bem como a natureza e a gravidade da ofensa, com conseguinte averiguação da capacidade da situação gerar uma afetação anímica para a vítima. Recorda-se, nesse ponto, a grave conjuntura ocasionada pela dispensa discriminatória outrora mencionada, a qual distancia-se, em termos de gravidade, quanto a criação de estereótipos tidos como de menor porte ofensivo. Ensejando, pois, *quantuns* compensatórios distintos.

Outrossim, o autor acrescenta que um outro elemento que merece análise para o estabelecimento do quantum indenizatório é o prolongamento temporal dos danos. Os quais podem ser temporários, cuja ocorrência se esgota no tempo, ou permanentes, posto que se projetam por um longo e indefinido período.

Para o acesso indevido a dados sensíveis de saúde, esse critério tem peculiar interesse. Haja vista que, as consequências do vazamento de uma informação quanto a alguma vulnerabilidade mais gravosa do indivíduo pode ocasionar um processo de

---

323 COSTA, Mário Júlio Almeida. **Direito das obrigações**. Coimbra: Almedina, 2004, p. 554.

324 BRASIL. Superior Tribunal de Justiça. **RESP: 1.152.541 – RS.** Relator: Ministro Paulo de Tarso Sanseverino. Data de Julgamento: 13/09/2011. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201101071104&dt_publicacao=29/02/2012. Acesso em: 29 maio 2024.

325 MIRAGEM, Bruno. **Responsabilidade Civil**. Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 fev. 2024. p. 228.

estigmatização que se projete por muito tempo. O que deve ser levado em consideração para o estabelecimento do quantum indenizatório devido.

Ora, a estigmatização inerente ao acesso de uma informação vinculada ao acometimento por HIV, por exemplo, é completamente distinta do acesso a um dado vinculado a uma hipertensão arterial.

Logo, as projeções temporais e os potenciais de discriminação dos danos são completamente distintos. Requerendo, pois, uma dinâmica reparatória diferenciada. Note-se que aqui se impõe a observância da proporcionalidade para distinguir entre diversos danos decorrentes de lesão à personalidade e suas consequências concretas à vítima para uma adequada compensação.

Ademais, para além dos critérios apresentados, cabe acrescentar a observação quanto a capacidade econômica do ofensor. Miragem aponta que esse método atua para que a indenização também sirva como mecanismo de desestimulo para a reiteração da conduta ofensiva.

De modo que, atuaria como uma forma de prevenção para evitar novas projeções danosas por parte do ofensor ou de terceiros. Inclusive, analisando, se for o caso, o proveito do ofensor com a realização do dano, caso sua conduta seja em benefício próprio. Evitando, assim, a frustração do que o autor chamou de função dissuasória da indenização.

5 CONCLUSÃO

Diante do outrora exposto, em um evidente cenário de riscos e interesses que permeiam os dados sensíveis, a presente pesquisa ganha contornos significativos. Especialmente, quando setores mal intencionados violam informações pessoais em ataques a sistemas, ocasionando uma série de danos aos titulares dos dados e à prestação do serviço.

Organizações de saúde e demais instituições hospitalares estão entre os alvos mais atraentes dos invasores, já que os prontuários médicos possuem, em um único documento, quase tudo que o indivíduo mal intencionado precisa para realizar esquemas sofisticados de fraude. Esta que afeta desde o setor de seguros ao roubo total de identidade a ser utilizado em extorsões ou outras práticas irregulares. Os registros dos pacientes, portanto, são alvos lucrativos e mostram-se como ativos caros no mercado ilegal.

Assim, por um lado, a implantação de novos dispositivos tecnológicos oferece aos ambientes médicos recursos importantes para o aumento da eficiência no atendimento. Por outro, cada dispositivo aumenta a superfície de ataque de uma organização. Portanto, a produção de estratégias normativas e, principalmente, de mecanismos de responsabilização dos agentes envolvidos devem ser significativamente perseguidas.

Ora, uma adequada gestão dos dados pessoais mostra-se como fundamental, seja preventivamente ou como mecanismo compensatório. Já que atua como instrumento de salvaguarda não só das prerrogativas constitucionais inerentes à dignidade da pessoa humana, à privacidade, e à liberdade deliberativa do paciente, mas também envolvem aspectos inerentes à própria projeção do indivíduo.

O que, considerando um cenário social, no qual o indivíduo se projeta e constrói neste a sua auto delimitação, urge-se a estruturação de uma tutela cada vez mais contundente para que este possa ter autonomia ao se relacionar socialmente.

Já que proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade, sem discriminação de qualquer natureza, conforme orienta a própria constituição. Salvaguardando a possibilidade do indivíduo delimitar o conteúdo das informações, a seu respeito, que serão acessadas pelos seus pares.

Conforme discussões outrora suscitadas, a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.

Desse modo, determinados dados acabam sendo selecionados para terem um caráter de confidencialidade ainda mais acentuado. O que ocorre, por exemplo, com os dados de saúde, o qual guarda em seu bojo um conteúdo altamente passível de discriminação.

Exemplo evidencia-se com a própria questão da estigmatização outrora mencionada. Na qual, a sociedade estabelece os meios para caracterizar as pessoas, as dividindo em grupos vinculados aos atributos naturalmente perceptíveis. Que, quando se tratam de vertentes tidas socialmente como negativas, podem afetar diversas esferas relacionais, como o próprio ambiente de trabalho do titular dos dados.

Cabe, inclusive, retomar que o estigma ganha significado relacional[326] na atualidade, posto que conecta atributos e estereótipos a formas de estigmatização. Ocasionando os indesejados preconceitos, desaprovações ou discriminações embasadas em características, comportamentos ou identidades que são tidas, erroneamente, por indesejáveis ou reprováveis pela sociedade. Os quis podem culminar nos mais variados danos à esfera anímica do indivíduo.

Nesse cenário, justifica-se que os mencionados dados sensíveis de saúde, amplamente encontrados nos prontuários dos pacientes, compreendem uma tipologia distinta. Especialmente, em decorrência da natureza do seu conteúdo oferecer uma especial vulnerabilidade, nos moldes do outrora exposto. Dessa forma, existe a razoável preocupação em haver discriminação ou diferenciação de uma pessoa em detrimento de tais aspectos da sua personalidade.

Ademais, a notória preocupação com a salvaguarda desse preceito finca-se no pressuposto básico de que garantindo a proteção das informações pessoais atinentes ao paciente haveria, por conseguinte, a salvaguarda da lealdade profissional, enquanto fator que reforça a credibilidade de certas profissões, promovendo a confiança necessária para o bom funcionamento destas atividades.

---

[326] GOFFMAN, Erving. **Estigma: la identidade deteriorada**. 5.ed. Buenos Aires: Amorrortu Editores, 1993. p. 11.

De modo que, normalmente, o convívio em sociedade gera a necessidade de valer-se do auxílio de terceiros, os quais, por vezes, possuem acesso a fatos íntimos, que o indivíduo almejava manter em segredo, em prol da resolução de alguma vertente de problema.

Nesse sentido, determinados segmentos profissionais são consagrados como *confidentes necessários*, isto é, no suceder do exercício de seus trabalhos, esses profissionais tem contato direto com informações de caráter íntimo e confidencial. A exemplo de advogados, psicólogos, médicos e até mesmo padres que testemunham verdadeiras confissões de pecados. Assim, é evidente que os profissionais, em diferentes níveis, devem proteger as informações reveladas no exercício profissional.[327]

À vista disso, faz-se fundamental a salvaguarda do sigilo profissional, com o intuito de assegurar o uso desses serviços de modo eficiente e resguardado, com a proteção de poder expor confidências íntimas, sem o perigo de vê-las reveladas, gerando, por consequência, futuros constrangimentos.

Nesse cenário, no qual as organizações de saúde e demais instituições hospitalares estão entre os alvos mais atraentes dos invasores, bem como considerando a relevância e a interferência dos dados sensíveis veiculados nessa relação, surge a presente pesquisa. Especialmente, considerando uma conjuntura de ataques extremamente atuais.

A exemplo do ocorrido envolvendo um grupo de cibercriminosos, o qual sequestrou e divulgou dados financeiros, imagens íntimas e outras informações pessoais de pacientes atendidos por um consultório de cirurgia plástica do Rio Grande do Sul e do Paraná”[328]. Os danos inerentes à vertente exposição atingiram proporções significativas, as quais dariam vasta discussão.

A publicação em questão, segundo a mídia, fora materializada pelo grupo Qiulong na *deep web* e constou de um pedido de resgate visando a não divulgar do resto dos dados nas redes sociais.

A ação da organização foi identificada pela empresa ISH Tecnologia no dia 22 de abril de 2024. Este incidente destaca a sofisticação e a audácia crescentes de ataques

---

[327] DE PAULA, Alexandre Sturion. Digressões sobre a violação do sigilo profissional. **Portal Universo Jurídico**, 2002. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/10736-10736-1-PB.htm. Acesso em: 30 nov. 2023.

[328] GLOBO. Ameaças e pedidos de resgate: Hackers vazam imagens de pacientes nus de clínica de cirurgia plástica do Sul. **O Globo**, 2024. Disponível em: https://oglobo.globo.com/brasil/noticia/2024/04/29/hackers-vazam-imagens-de-pacientes-nus. Acesso em: 18 jun. 2024.

ransomware no setor da saúde, um dos setores mais visados por esse tipo de crime no Brasil. Trazendo mais uma relevante preocupação quanto a salvaguarda adequada dos sistemas de armazenamento de dados, bem como a presença de um adequado e robusto sistema de responsabilização.

Ressalta-se que o vertente estudo objetivou analisar um recorte voltado para a responsabilidade civil do hospital decorrente do acesso indevido a dados sensíveis de saúde do paciente. A qual, por uma perspectiva sistêmica do ordenamento jurídico, concluiu-se pela aplicação da responsabilidade objetiva à instituição hospitalar, mas não irrestrita.

Para tanto, trousse a lume a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor, vários apontamentos jurisprudenciais e vasta doutrina especializada sobre o tema. Considerando, em tomada antecedente, a aplicação de um relevante recorte, segundo o qual fora analisada a responsabilidade da instituição por atos extramédicos[329]. Isto, ante a complexidade inerente a uma estrutura hospitalar[330].

Os fundamentos para pautar processo indenizatório por uma reparação objetiva são diversos, mas cabe pontuar algumas das reflexões realizadas. Por um lado, tem-se na figura do paciente o enquadramento como usuário final do serviço prestado[331]. Inserido, pois, no conceito de consumidor, cabendo aos outros partícipes dessa relação complexa, a função de fornecedores do serviço de saúde prestado pela instituição hospitalar.

Por outro lado, para alguns autores[332], não seria forçoso admitir, ao menos enquanto regra, a mencionada objetivação na reparação conferida aos agentes responsáveis pelo tratamento dos dados, mesmo que a LGPD não tenha disposto explicitamente quanto à natureza da responsabilidade dos agentes de tratamento de dados.

Assim, assume-se que a culpa prescinde de demonstração, mas a comprovação da adequada existência do dano e de um nexo causal intacto se mostra extremamente devida, com respaldo na própria teoria geral da responsabilidade civil. Essa disposição sana a aparente dubiedade entre as redações dos artigos 44 e 42 da LGPD.

---

[329] Normalmente, a responsabilidade hospitalar pode ser dividida em três macro setores, dentre os quais encontram-se as reparações por atos médicos, paramédicos e extramédicos.
[330] Posto a existência de diversas atividades distintas sendo desempenadas em um mesmo espaço.
[331] Consoante a exegese do art. 2º do CDC.
[332] TASSO, Francisco Augusto. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

Posto que, este último dispositivo impõe a obrigação de indenizar "em razão do exercício de atividade de tratamento de dados pessoais", fundamentando a prescindibilidade da análise de culpa.

Ao passo que o art. 44[333] da LGPD vincula-se à ideia de defeito na prestação do serviço, determinando a obrigação de indenizar caso ocorra tratamento irregular de dados pessoais. O que encontra-se diretamente associado à necessária existência do nexo causal entre o dano experimentado pela vítima e o tratamento do dado.

Passou-se então a uma análise quanto aos possíveis rompimentos da cadeia causal, os quais, atuando de forma exclusiva, afastariam o dever de indenizar. Considerando, para tanto, a perspectiva trazida pelo art. 43 da LGPD, o qual funda-se na expressa exclusão da responsabilização diante da ocorrência devidamente provada de fato exclusivo de terceiro ou do titular dos dados[334].

Debatendo-se, mais, que a não adoção dos parâmetros normativos e técnicos existentes, eleva de modo considerável o risco inerente à prática do tratamento de dados. O que ocasiona um evidente risco interno da prática, posto que tal incremento parece estar associado a adoção de uma postura contrária à efetivação de práticas e técnicas efetivamente seguras no âmbito das operações com dados.

Nesse ponto, coube distinguir o vertente caso da perspectiva trazida pelo surgimento posterior de um mecanismo de acesso indevido a uma estrutura de armazenamento de dados, cujos fundamentos técnicos encontravam-se altamente respaldados pelos parâmetros de segurança existentes.

De modo que, concluiu-se por não parecer adequada a concepção genérica de que a invasão de sistemas e bases de dados por terceiros atuaria como um fortuito interno inerente ao risco da atividade a justificar a manutenção do processo de responsabilização. Para tanto, foram analisadas algumas distinções relevantes entre a invasão do sistema e o

---

[333] Esse dispositivo orienta sobre o que seria um tratamento irregular a ferir o dever de segurança na tutela do dado. Dispondo, mais, que a irregularidade em questão deve ser analisada sob a ótica de determinadas circunstâncias legalmente previstas. Dentre as quais, o modo de realização do tratamento dos dados, o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
Ressalta-se, mais, que o risco razoavelmente esperado encontra-se intimamente conectado com o dever da instituição de notificar de modo claro, amplo e inequívoco o paciente, quanto às questões inerentes a essa modalidade de gestão das informações pessoais necessárias à prestação do serviço. Adquirindo, assim, o consentimento livre e esclarecido do titular dos dados sensíveis.

[334] Nesse ponto, outras projeções contundentes foram realizadas não apenas quando da análise no âmbito da responsabilidade proposta pela LGPD, mas também ao realizar um aprofundamento quanto às disposições próprias ao estudo do nexo de causalidade.

vazamento dos dados, delineando alguns contornos normativos e standards de segurança da informação.

O vazamento de dados, também conhecido como "*data leak*", ocorre quando informações confidenciais são acidentalmente ou intencionalmente expostas a indivíduos ou organizações que não possuem autorização para acessá-las. Permitindo que criminosos cibernéticos obtenham acesso não autorizado aos dados confidenciais sem esforço[335].

Normalmente, o incidente em comento está atrelado a erros humanos, como envio de informações confidenciais para um e-mail incorreto ou por meio de falhas nos sistemas de armazenamento de dados[336].

Por outro lado, uma invasão de dados, ou "*data breach*" ocorre quando informações confidenciais são acessadas por indivíduos ou organizações não autorizados[337], tratando, pois, de uma violação dos dados. Durante essa ocorrência, a segurança dessas informações é violada, as deixando disponíveis para pessoas, usualmente, mal-intencionadas.

O incidente de Segurança em questão é mais comum em ataques cibernéticos, no qual *hackers* invadem sistemas de armazenamento de dados e roubam informações valiosas, que podem ser relativas a dados de saúde ou demais questões sensíveis. Uma violação de dados[338], portanto, é um incidente em que informações são roubadas ou retiradas de um sistema sem o conhecimento ou autorização do proprietário do sistema.

Coube dispor, mais, quanto a questões inerentes ao dever do fornecimento da segurança que legitimamente se espera do tratamento de dados de cunho sensível. Especialmente pontuando pontos cruciais quanto à legitima expectativa versada.

Delineando, também, quanto ao dever dos agentes envolvidos na operação com dados pessoais de prestar uma informação clara e de fácil acesso ao titular dos dados tratados, a qual considere, inclusive, a disposição quanto a existência de riscos no tratamento do dado em meio virtual.

---

[335] TUNGGAL. Allan Toh. What is a Data Leak? Stop Giving Cybercriminals Free Access. **UpGuard,** 2023. Disponível em: https://www.upguard.com/blog/data-leak. Acesso em: 26 dez. 2023.

[336] A exemplo do vazamento de senhas do Ministério da Saúde, o qual deixou exposto na internet dados pessoais e médicos de ao menos 16 milhões de brasileiros que tiveram diagnósticos suspeitos ou confirmados de COVID-19 (FCQ Advogados, 2020).

[337] AMORIM, Allex. Diferenças do Data Leak e Data Breach. **Linkedin**, São Paulo, 09 de março de 2023. Disponível em: https://pt.linkedin.com/pulse/diferenças-do-data-leak-e-breach-alex-amorim. Acesso em: 28 dez. 2023.

[338]HOLMES, D. What is Data Breach? **Fortnet,** 2023. Disponível em: https://www.fortinet.com/resources/cyberglossary/data-breach. Acesso em: 28 dez 2023.

Trabalhando, assim, com o aspecto dos níveis de risco normais e previsíveis[339]. Os quais são abstratamente auferíveis e amplamente conhecidos, especialmente quando a prestação do serviço perpassa pelo meio digital, ainda que apenas no que concerne à gestão de dados de cunho pessoal.

Considerando, mais, que a oferta de riscos anormais se enquadra no conceito de prestação defeituosa, esta enseja, portanto, a responsabilidade objetiva do fornecedor. Nesse interim, quando for imputado ao agente[340] um dever de prevenir a ocorrência de danos, especialmente nos casos em que a sua conduta der causa a riscos, tidos como anormais, a direitos ou interesses alheios, aquele deve responder pelos que der causa.

O mesmo ocorre com a inobservância dos preceitos normativos e dos standards técnicos voltados ao estabelecimento de um tratamento adequado dos dados pessoais. Os quais respaldariam uma concorrência entre o autor do dano e a instituição responsável por reparar a vítima. Assim, a não comprovação da concreta regularidade na tutela do sistema deflagra o dever de suportar a condenação nos moldes determinados pelo magistrado.

Desse modo, para que o hospital não seja responsabilizado é extrema relevância a comprovação de que a conduta do terceiro, *hacker*, não foi facilitada por nenhum descumprimento de padrões de segurança, seja normativo ou técnico. Evidenciando a ocorrência de um fortuito externo capaz de romper com o nexo causal entre a inação do hospital e o dano.

Assim, partindo das disposições outrora trazidas, nos casos em que a mencionada invasão por fato de terceiro decorreu, em verdade, de falha na prestação de segurança do serviço ou não fora realizada a notificação adequada dos pacientes quanto aos riscos inerentes ao canal de atendimento, os agentes do tratamento de respondem solidariamente pelos danos causados. Consoante a disposição amplamente analisada art. 42, §1º, II da LGPD[341].

Caso conclua-se pela inobservância dos preceitos legais ou inaplicação dos standards de segurança mínimos, caracterizando a ocorrência de um dano evitável, tem-se

---

[339] Art. 8º do CDC.

[340] Para a análise em questão, o agente é o controlador de dados sensíveis dos pacientes. Atuando como prestador do serviço de proteção dos dados na esfera hospitalar.

[341] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

a manutenção do dever de indenizar por parte do hospital. Podendo, a depender das circunstâncias fáticas, ensejar uma redução no quantum indenizatório devido.

Levando-se em consideração os precedentes jurisprudenciais, as condições sociais e econômicas das partes, o ilícito, a inexistência de enriquecimento sem causa do autor e o impacto gerado à instituição hospitalar para dissuadi-la a adoção de práticas de segurança mencionadas.

REFERÊNCIAS

ALEXY, Robert. **Teoría de los Derechos Fundamentales**. Madrid: Centro de Estúdios Políticos y Constitucionales, 2002.

ALMEIDA, Maria; MUNHOZ, Damião Rodrigues. O princípio e as razões do segredo médico. **Revista IMESC**, São Paulo, n.1, dez. 1998.

ALVIM, Agostinho Neves de Arruda. **Da inexecução das obrigações e suas consequências**. 4. ed. São Paulo: Saraiva, 1972.

AMORIM, Allex. Diferenças do Data Leak e Data Breach. **Linkedin**, São Paulo, 09 de março de 2023. Disponível em: https://pt.linkedin.com/pulse/diferenças-do-data-leak-e-breach-alex-amorim. Acesso em: 28 dez. 2023.

ANDRADE, Walmar Andrade. **A guarda de registros de conexão e de acesso a aplicações, conforme o Marco Civil da Internet**. Disponível em: https://walmarandrade.com.br/guarda-de-registros/#:~:text=Os%20registros%20de%20conex%C3%A3o%20e,conex%C3%A3o%20do%20usu%C3%A1rio%20%C3%A0%20internet. Acesso em: 22 mar. 2024.

ARAMPATZIS, Anastasios. Cibersegurança e conformidade para organizações da saúde. **Tripwire**, 2021. Disponível em: https://www.tripwire.com/state-of-security/healthcare/cybersecurity-and-compliance-for-healthcare-organizations/. Acesso em: 26 dez. 2023.

ASCENSÃO, José de Oliveira. **Teoria Geral do Direito Civil**. Coimbra: Editora Coimbra, 1997.

ASSOCIATED PRESS. Ataque hacker interrompe funcionamento de hospitais nos Estados Unidos e FBI abre investigação. **Globo**, 2023. Disponível em: https://g1.globo.com/tecnologia/noticia/2023/08/10/ataque-hacker-interrompe-funcionamento-de-hospitais-nos-estados-unidos-e-fbi-abre-investigacao.ghtml. Acesso em: 05 jan. 2024.

BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo – a construção de um conceito jurídico à luz da jurisprudência mundial**. Belo Horizonte: Fórum, 2014.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo**. 5. ed. São Paulo: Saraiva, 2015.

BASTOS, Celso Ribeiro Bastos. **Curso de direito constitucional**. São Paulo: Saraiva, 1997.

BASTOS, Celso Ribeiro Bastos. Tribunal Regional Federal da 1ª Região. **A Constituição na Visão dos Tribunais - Interpretação e Julgados - Artigo por Artigo**. v. 1. Brasília: Editora Saraiva, 1997.

BELTRÃO, Silvio Romero. Direito da Personalidade: Natureza Jurídica, Delimitação do Objeto, Relações com o Direito Constitucional. *In:* MENEZES, Joyceane Bezerra. (Org.). **Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira**. 1 ed. Florianópolis: Conceito, 2010, v. 1, p. 471-489.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Forense, 2019.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 2. ed. Rio de Janeiro: Forense Universitária, 1995.

BRASIL. **Constituição (1988).** Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 29 maio 2024.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Diário Oficial da União, Poder Executivo, Brasília, DF, 31 dez. 1940. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 maio 2024.

BRASIL. **Emenda Constitucional nº 115, de 15 de dezembro de 2022**. Altera os arts. 21, 40, 201, 203 e 204 da Constituição Federal para dispor sobre o novo regime de previdência complementar dos servidores públicos. Diário Oficial da União: seção 1, Brasília, DF, 16 dez. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=Emenda%20Constitucional%20n%C2%BA%20115&text=Altera%20a%20Constitui%C3%A7%C3%A3o%20Federal%20para,e%20tratamento%20de%20dados%20pessoais. Acesso em: 29 maio 2024.

BRASIL. Instituto Nacional de Tecnologia da Informação. ICP-Brasil. **Gov.br**, 2023. Disponível em: https://www.gov.br/iti/pt-br/assuntos/icp-brasil. Acesso em: 01 jan. 2024.

BRASIL. **Lei n. 13.787, de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 01 jan. 2024.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 maio 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 29 maio 2024.

BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Diário Oficial da União,
Brasília, DF, 17 mar. 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 29 maio 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).**
Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 29 maio 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 29 maio 2024.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: Maria Edite de Souza. Processual Civil e Administrativo. Indenização por Dano Moral. Vazamento de Dados Pessoais. Dados Comuns e Sensíveis. Dano Moral presumido. Impossibilidade. Necessidade de Comprovação do Dano. Relator: Min. Francisco Falcão, 07 mar. 2023. Disponível em:https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28ARESP.clas.+e+%40num%3D%222130619%22%29+ou+%28ARESP+adj+%222130619%22%29.suce.&O=JT. Acesso em: 03 mar 2023.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Relator: Min. Francisco
Falcão, 07 mar. 2023. Disponível em:https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28ARESP.clas.+e+%40num%3D%222130619%22%29+ou+%28ARESP+adj+%222130619%22%29.suce.&O=JT. Acesso em: 03 mar 2023.

BRASIL. Superior Tribunal de Justiça. **AREsp: 2008070 SP 2021/0356249-0**. Rel. Min. Luis Felipe Salomão. DJe 08/02/2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1373329300. Acesso em: 29 maio 2024.

BRASIL. Superior Tribunal de Justiça. **EDcl no AREsp 2490156**. Rel. Min. Maria Isabel Gallotti. Brasília, DF, 07 mai. 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 971.845/DF**. Rel. Nancy Andrighi. Diário da

Justiça Eletrônico, nº 269, de 01/12/2008. Disponível em:https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200701573821&dt_publicacao=01/12/2008#:~:text=Trata%2Dse%20de%20recurso%20especial,de%20SERVIER%20DO%20BRASIL%20LTDA. Acesso em: 29 maio 2024.

BRASIL. Superior Tribunal de Justiça. **RESP: 1.152.541 – RS**. Relator: Ministro Paulo de Tarso Sanseverino. Data de Julgamento: 13/09/2011. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201101071104&dt_publicacao=29/02/2012. Acesso em: 29 maio 2024.

BRASIL. Supremo Tribunal Federal. **O método bifásico para fixação de indenizações por dano moral.** Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-10-21_06-56_O-metodo-bifasico-para-fixacao-de-indenizacoes-por-dano-moral.aspx. Acesso em: 05 abr 2024.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 1375558/AC.** Direito Constitucional. Prontuários médicos de pacientes atendidos na rede pública estadual. Documento de natureza sigilosa. Requisição direta pelo Ministério Público do Estado para fins de investigação criminal. Impossibilidade. Reserva de Jurisdição. Direito à Intimidade. Recurso Extraordinário a que se nega seguimento. Relatora: Min. Rosa Weber, 02 set. 2022. Diário de Justiça, nº 179, divulgado em 08 set. 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6373575. Acesso em: 05 dez 2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6387.** Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 29 maio 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6388**. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357772. Acesso em: 29 maio 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6389**. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1. Acesso em: 29 maio 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6390**. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1.Acesso em: 29 maio 2024.

BRASIL. Supremo Tribunal Federal. **AREsp: 2547642**, Relator: Ministra Maria Thereza de Assis Moura,
Data de Publicação: 25/04/2024 Disponível em:https://www.jusbrasil.com.br/jurisprudencia/stj/2482880174/inteiro-teor-2482880177

BRASIL. Tribunal Superior do Trabalho. **Súmula nº 443.** Presunção de dispensa discriminatória. Diário da
Justiça [da] República Federativa do Brasil. Disponível em: https://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_401_450.html. Acesso em: 29 maio 2024.

CAPELO DE SOUSA, Rabindranath Valentino Aleixo. **O direito geral de personalidade**. Coimbra: Coimbra Editora, 2011.

CASADO FILHO, Napoleão. **Direitos humanos fundamentais**. São Paulo: Saraiva, 2012.

COHEN, Julie. Examined Lives, Informational Privacy and the Subject as Object. **Stanford Law Review**, v. 52, p. 1373-1438, 2000.

CONSELHO FEDERAL DE MEDICINA (CFM). **Código de Ética Médica**. Brasília, DF: CFM, 2018. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 29 maio 2024.

CONSELHO FEDERAL DE MEDICINA (CFM). Fiscalização: CFM estabelece regras mínimas para serviços
de assistência médica. **Portal CFM**, Brasília, 12 nov. 2013. Disponível em: https://portal.cfm.org.br/noticias/fiscalizacao-cfm-estabelece-regras-minimas-para-servicos-de-assistenciamedica/#:~:text=Registro%20de%20prontu%C3%A1rios%20%E2%80%93%20Os%20hospitais%20tamb%C3%A9m%20ter%C3%A3o,demais%20profissionais%20de%20sa%C3%BAde%20que%20intervenham%20na%20assist%C3%AAncia. Acesso em: 01 jan. 2024.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 1.638, de 10 de julho de 2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários. nas instituições de
saúde Brasília: CFM, 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 01 dez. 2023.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução n. 2. 218, de 29 de novembro de 2018**. Revoga o artigo 10º da Resolução CFM nº 1.821/2007, de 23 de novembro de 2007. Brasília: CFM, 2018. Disponível em:
https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2218. Acesso em: 01 jan. 2024.

CORDEIRO, Antônio Menezes. **Tratado de Direito Civil Português**. Coimbra: Almedina, 2007.

COSTA JÚNIOR, Paulo José. **Nexo causal**. 3. ed. São Paulo: Siciliano Jurídico, 2004.

COSTA, Mário Júlio Almeida. **Direito das obrigações**. Coimbra: Almedina, 2004.

COUTINHO, Rogério. Inca cancela consultas e exames após sistema sofrer invasão hacker; não há
previsão de retorno. **Globo**, 2024. Disponível em: https://g1.globo.com/rj/rio-de-

janeiro/noticia/2024/01/29/sistema-do-inca-sofre-invasao-hacker.ghtml. Acesso em: 26 mar. 2024.

COUTO, José Henrique Oliveira. Vazamentos De Dados E Dano Moral 'In Re Ipsa': Comentários Ao Agravo Em Recurso Especial Nº 2.130.619/Sp. **Revista IBERC**, v. 06, n. 02, p. 171-188, mai./ago. 2023. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/52/42. Acesso em: 28 dez. 2023.

CRUZ, Gisele Sampaio da. **O problema do nexo causal na responsabilidade civil.** Rio de Janeiro: Renovar, 2005.

CRUZ, Natalia. Estigma Social**:** O Que é, Significado e Estigmatização. **Quero Bolsa**, 2022. Disponível em: https://querobolsa.com.br/enem/sociologia/estigma-social. Acesso em: 15 nov. 2023.

CRYPTOID. **Relatório do Cenário de Ameaças da Tenable: Brasil é o país com o maior volume e dados expostos no mundo**. Disponível em: https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/relatorio-do-cenario-de-ameacas-da-tenable-brasil-e-o-pais-com-o-maior-volume-e-dados-expostos-no-mundo/. Acesso em: 08 jan. 2024.

DE PAULA, Alexandre Sturion. Digressões sobre a violação do sigilo profissional. **Portal Universo Jurídico**, 2002. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/10736-10736-1-PB.htm. Acesso em: 30 nov. 2023.

DELGADO, Mauricio Godinho. **Curso de Direito do Trabalho**. 4. ed. São Paulo: LTr, 2005.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DOTTI, René Ariel. **Curso de direito penal**. Rio de Janeiro: Forense, 2001.

ETZIONI, Amitai. A Communitarian Approach: A Viewpoint on the Study of the Legal and Ethical Policy Considerations Raised by DNA Tests and Databases. **Journal of Law, Medicine & Ethics**, v. 34, 2006.

FALEIROS JÚNIOR, José Luiz de Moraes; NOGAROLI, Ricardo; CAVET, Carlos Alexandre. Telemedicina e proteção de dados: reflexões sobre a pandemia da COVID-19 e os impactos jurídicos da tecnologia aplicada à saúde. **Revista dos Tribunais** [recurso eletrônico]. São Paulo, n. 1016, jun. 2020. Disponível em: https://dspace.almg.gov.br/handle/11037/37577. Acesso em: 26 out. 2023.

FARINA, Arnaldo. Prontuário Médico. **Portal CFM**, 1999. Disponível em: https://portal.cfm.org.br/artigos/prontuario-medico/. Acesso em: 05 jan. 2024.

FCQ ADVOGADOS. **Vazamento de dados no Ministério da Saúde expõe informações pessoais de 16 milhões de pacientes.** 2020. Disponível em:

https://www.fcqadvogados.com/vazamento-de-dados-no-ministerio-da-saude-expoe-informacoes-pessoais-de-16-milhoes-de-pacientes/. Acesso em: 28 dez. 2023.

FEEGOW. **O que é backup do sistema e como fazer o da sua clínica?** 2020. Disponível em: https://feegowclinic.com.br/backup-do-sistema-blog/. Acesso em: 08 jan. 2024.

FERNANDES, Mário Sérgio. Prontuário eletrônico e a lei geral de proteção de dados. **Migalhas**, 02 fev. 2020b. Disponível em: https://www.migalhas.com.br/coluna/migalhas-deprotecao-de-dados/340202/prontuario-eletronico-e-a-lei-geral-de-protecao-de-dados. Acesso em: 09 dez. 2023.

FRANÇA, Genival Veloso de. **Direito médico**. 12. ed., rev., atual., e ampl. Rio de Janeiro: Forense, 2014.

FREDA, André. O que é um ataque de dia zero? **Avast**, 2021. Disponível em: https://www.avast.com/pt-br/c-zero-day. Acesso em: 05 jan. 2024.

FUENTES, Maricel Rivera; HUQ, Nashid. **Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks**. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf. Acesso em: 26 abr. 2024.

GOFFMAN, Erving. **Estigma: la identidade deteriorada**. 5.ed. Buenos Aires: Amorrortu Editores, 1993.

GOFFMAN, Erving. **Estigma - notas sobre a manipulação da identidade deteriorada**. Tradução em 2004. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mprj.mp.br/documents/20184/151138/goffman,erving.estigma_notassobreamanipulacaodaidentidadedeteriorada.pdf. Acesso em: 05 abr. 2024.

GONÇALVES, Carlos Roberto. Responsabilidade Civil. 18ª edição. São Paulo: Saraiva, 2023. E-book. ISBN 9786553624450. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553624450/. Acesso em: 15 dez. 2023.

GONÇALVES, Diogo Costa. **Pessoa e direitos da personalidade: fundamentação ontológica**. Coimbra: Almedina, 2008, p. 40-60.

GONÇALVES, José Luiz Ramalho. Algumas considerações sobre segredo médico e segredo profissional de advogado (em Portugal e no Brasil). **Revista CEJ**, v. 3 n. 7 jan./abr. 1999, p. 100-107. Disponível em: https://revistacej.cjf.jus.br/cej/index.php/revcej/article/view/184/346. Acesso em: 11 dez. 2023.

GOOGLE CLOUD. **Criptografia em trânsito.** 2024**.** Disponível em:https://cloud.google.com/docs/security/encryption-in-transit?hl=pt-br. Acesso em: 08 jan. 2024.

GRECO, Leonardo. **O processo de execução**. Rio de Janeiro: Renovar, 1999.

GUEDES, Gustavo Siqueira da Costa; MEIRELES, Roberta Motta Veloso. **Término do tratamento de dados.** In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Maria de Fátima. Lei Geral de Proteção de Dados Pessoais. São Paulo: Editora RT, 2019.

HERRERA, Edgardo López. **Teoría general de la responsabilidad civil**, cit., p. 202; HONORÉ, A. M. Causation and remoteness of damage, cit., p. 38-39.

HOLMES, David. What is Data Breach? **Fortnet,** 2023. Disponível em:https://www.fortinet.com/resources/cyberglossary/data-breach. Acesso em: 28 dez 2023.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Transparência e Governança nos algoritmos, um estudo de caso sobre o setor de birôs de crédito.** Rio de Janeiro: ITS, 2017. Disponível em https://itsrio.org/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf. Acesso em: 15 nov. 2023.

INSTITUTO DE TECNOLOGIA E SOCIEDADE. **Transparência e Governança nos algoritmos, um**
estudo de caso sobre o setor de birôs de crédito. Disponível em: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://d26k070p771odc.cloudfront.net/wp-content/uploads/2017/05/algorithm-transparency-and-governance-pt-br.pdf. Acesso em: 5 abr. 2024.

INTERNATIONAL BUSINESS MACHINES CORPORATION (IBM BRASIL). **Autenticação de camada de mensagem**. 2023. Disponível em: https://www.ibm.com/docs/pt-br/was-nd/8.5.5?topic=mechanism-message-layer-authentication. Acesso em: 08 jan. 2024.

KACHANI, Morris. Ou a sociedade acompanha internet ou a democracia começa a ficar em xeque. **Folha de São Paulo**. 2014. Disponível em: http://blogdomorris.blogfolha.uol.com.br/2014/04/08/ou-sociedade-acompanha-internet-ou-democracia-comeca-a-ficar-em-xeque/. Acesso em: 26 jun. 2021.

KASPERSKY. **O que é engenharia social?** 2023. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 08 jan. 2024.

KASPERSKY. **Ransomware: definição, prevenção e remoção**. 2023. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 08 jan. 2024.

KASPERSKY. **What is the cost of data breach**? In: Kaspersky blog. s.l: 2018. Disponível em: https://www.kaspersky.com/blog/economics-report-2018/22486/. Acesso em: 11 jan. 2024.

KFOURI, Maurício Zanoide de Moraes. **Responsabilidade Civil dos Hospitais - Código Civil e Código de Defesa do Consumidor.** São Paulo: Thomson Reuters Revista dos Tribunais, 2022. RB-1.1. Ebook. ISBN 9786559910489. Disponível em:https://nextproview.thomsonreuters.com/launchapp/title/rt/monografias/105155050/v5/page/RB-1.1%20. Acesso em: 22 nov. 2023.

KONDER, Carlos Nelson; MORAES, Maria Celina Bodin de. **Dilemas de direito civil-constitucional: casos e decisões**. Rio de Janeiro: Renovar, 2012.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. **Private traits and attributes are predictable from digital records of human behavior**. 2013. Disponível em: http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html. Acesso em: 15 nov. 2023.

LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003.

LIBERAL, Horácio Silva Pires. Sigilo Profissional. **Portal CFM**, 1993. Disponível em: http://www.portalmedico.org.br/include/biblioteca_virtual/des_etic/10.htm. Acesso em: 29 dez. 2023.

LIMA, Eduardo Picanço Pinto de Souza. Daños por violación de los deberes informativos del consentimiento informado. **Revista IBERC**, v. 02, n. 02, p. 01-19, mai./ago. 2019. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/52/42. Acesso em: 15 out. 2023.

LÔBO, Paulo. **Direito Civil: parte geral**. São Paulo: Saraiva, 2015.

LOCH, Jacqueline Azevedo. Confidencialidade: natureza, características e limitações no contexto da relação clínica. **Revista Bioética**. Brasília. v. 11. p. 51-64. nov. 2003. Disponível em: https://revistabioetica.cfm.org.br/revista_bioetica/article/view/149/153. Acesso em: 11 dez. 2023.

MACKAAY, Ejan. ROUSSEAU, Stefan. **Análise Econômica do Direito**. São Paulo: Editora Atlas, 2015.

MARCON, Daniele Vidal. Dano moral e vazamento de dados: o STJ escreveu certo por linhas tortas? **Consultor Jurídico**, abr. 2023. Disponível em: https://www.conjur.com.br/2023-abr-09/daniele-marcon-dano-moral-vazamento-dados/. Acesso em: 24 nov. 2023.

MARTINS, Flávio José Barbosa. **Dignidade da pessoa humana – princípio constitucional fundamental**. Curitiba: Juruá, 2003, p. 102-103.

MIRAGEM, Bruno. **Responsabilidade Civil.** Rio de Janeiro: Grupo GEN, 2021. E-book. ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 22 fev. 2024.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 555, 2018. Disponível em: https://www.revistadedireitodoconsumidor.com.br/. Acesso em: 05 jun. 2024.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. **Redes sociais virtuais, privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet**. Revista Pensar, v. 21, n. 1 2017.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18). *In:* MARTINS, Gustavo. M.; ROSENVALD, Nelson. (Org.). **Responsabilidade civil e novas tecnologias**. 1ed. Belo Horizonte: Editora Foco, 2020, v. 1, p. 109-124. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf. Acesso em: 15 nov. 2023.

JORGE NETO, Francisco Ferreira; CAVALCANTE, José de Queiroz Pereira. **Direito do Trabalho**. 7. ed. São Paulo: Atlas, 2013.

O GLOBO. **Ameaças e pedidos de resgate: Hackers vazam imagens de pacientes nus de clínica de cirurgia plástica do Sul.** 2024. Disponível em: https://oglobo.globo.com/brasil/noticia/2024/04/29/hackers-vazam-imagens-de-pacientes-nus-de-clinica-de-cirurgia-plastica-do-sul-e-prontuarios-de-saude-sexual.ghtml. Acesso em: 07 maio 2024.

O GLOBO. **Funcionário do Einstein vaza dados do Ministério da Saúde e expõe 16 milhões de pacientes com Covid-19.** 26 nov. 2020. Disponível em: https://oglobo.globo.com/brasil/funcionario-do-einstein-vaza-dados-do-ministerio-da-saude-expoe-16-milhoes-de-pacientes-com-covid-19-24766745 Acesso em: 01 dez. 2023.

OBASTIDOR. **Hackers invadem sistemas de hospitais públicos de Brasília**. https://obastidor.com.br/investigacao/hackers-invadem-sistemas-de-hospitais-publicos-de-brasilia-2119. Acesso em: 08 mar. 2024.

OLIVEIRA, Rodrigo da Costa de. Direito a intimidade e sua proteção baseada nos direitos humanos no mundo. **Âmbito Jurídico**. 2014. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/direito-a-intimidade-e-sua-protecao-baseada-nos-direitos-humanos-no-mundo/#_ftn7. Acesso em: 28 dez. 2023.

PEREIRA, Caio Mário da Silva. **Obrigações e contratos – pareceres**, Rio de Janeiro: Forense, 2011.

PEREIRA. Caio Mário da Silva**. Instituições de Direito Civil.** Rio de Janeiro: Forense, 2022. v.3.

PERROTTI, Paulo. Saúde: clínicas são as que mais sofrem com ataques cibernéticos. **Solution Hub**. 2023. Disponível em: https://solutionhub.com.br/saude-clinicas-sao-as-que-mais-sofrem-com-ataques-ciberneticos/. Acesso em: 18 abr. 2024.

PIERANGELI, José Henrique. **Manual de direito penal brasileiro, v. 2: parte especial: arts. 121 a 361**. 2. ed. rev., atual., ampl. e compl. São Paulo: Editora Revista dos Tribunais, 2007, p. 187-188.

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de direito privado**. 3. ed. Rio de Janeiro: Editor Borsoi, 1971. v. 22.

REALE, Miguel. **Filosofia do direito**. São Paulo: Saraiva, 2002. p. 208-214.

RÊGO, Isabelle Souza Ulisses. **Telemedicina**: análise sobre a responsabilidade civil do terceiro no tratamento indevido de dados sensíveis do paciente. 2021. 73f. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Piauí, Teresina, 2021.

RODOTÀ, Stefano. **A vida na Sociedade de Vigilância**: privacidade hoje, Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson. **A Responsabilidade Civil pelo Ilícito Lucrativo**. 2 ed. Salvador: Juspodvim, 2021.

ROSENVALD, Nelson; CORREIA, Anderson; MONTEIRO FILHO, Carlos Eduardo do Rêgo; KHOURI, Paulo Roberto. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais--culpa-ou-risco. Acesso em: 26 dez. 2021.

SANTIAGO, Luiz Carlos Figueiredo. O sigilo médico e o direito penal. **Revistas UNIFACS**, Salvador, n. 128, fev. 2011. Disponível em: https://revistas.unifacs.br/index.php/redu/article/viewFile/1409/1096. Acesso em: 29 nov. 2023.

SANTOS, Ricardo. Prejuízo por vazamentos de dados deve ser provado para justificar dano moral. **Consultor Jurídico**. 2021. Disponível em: https: https://www.conjur.com.br/2021-jun-22/vazamento-dados-gera-indenizacao-dano-for-provado. Acesso em: 11 out. 2023.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. 5ª Câmara de Direito Público**. Apelação Cível nº 10168440320208260068 SP**. Danos Morais. Danos Materiais. Divulgação De Prontuário Médico. Hiv.
Relatora: Heloísa Martins Mimessi. 07 de julho de 2021. Disponível em:https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2097727220/inteiro-teor-2097727224. Acesso em: 11 nov 2023.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. 5ª Câmara de Direito Público**. Apelação Cível nº 10168440320208260068 SP**. Danos Morais. Danos Materiais. Divulgação De Prontuário Médico. Hiv. Relatora: Heloísa Martins Mimessi. 07 de julho de 2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/2097727220/inteiro-teor-2097727224. Acesso em: 11 nov 2023.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental À Proteção De Dados. *In:* DONEDA, D. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 2.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2013. p. 135.

SECURITYLEADERS. **Hospital Universitário da USP confirma ataque hacker aos sistemas informatizados**. Disponível em: https://securityleaders.com.br/hospital-universitario-da-usp-confirma-ataque-hacker-aos-sistemas-informatizados-2/ Acesso em: 08 mar. 2024.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 41. ed., ver. e atual. São Paulo: Malheiros, 2018.

SILVA, Ernesto Tavares da. A responsabilidade do profissional da saúde na proteção dos dados pessoais de pacientes,
de acordo com a LGPD. **Migalhas**, 28 mar 2023. Disponível em: https://www.migalhas.com.br/amp/depeso/383751/profissional-da-saude-e-a-protecao-dos-dados-pessoais-de-pacientes. Acesso em: 09 dez. 2023.

SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE (SBIS). **O que é Certificação de S-RES SBIS.** 2023. Disponível em: http://sbis.org.br/certificacao-sbis/. Acesso em: 8 jan. 2024.

SOLOVE, Daniel. Data is what data does: regulating use, harm, and risk instead of sensitive data. **Northwestern University Law Review**, v. 118, jan. 2023, p. 35-36. Disponível em: https://ssrn.com/abstract=4322198. Acesso em: 11 nov 2023.

SOUZA, Paulo Vinícius Silva de. **Direito Penal Médico**. Porto Alegre: Livraria do Advogado Editora, 2009.

TASSO, Francisco Augusto. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

TAYLOR, Charles**. La ética de la autenticidad**. Barcelona: Paidos, 1994.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil - Vol. 4 - Responsabilidade Civil.** São Paulo: Grupo GEN, 2024. E-book. ISBN 9786559649563. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559649563/. Acesso em: 24 mar. 2024.

TEPEDINO, Gustavo; SPADACCINI, Chiara. O Consentimento na Circulação de Dados Pessoais. **Revista Brasileira de Direito Civil – RBDCivil**. Belo Horizonte, v. 25, p. 83-116, jul./set. 2020. Disponível em: https://www.rbdcivil.com.br/revista/edicao-25/o-consentimento-na-circulacao-de-dados-pessoais. Acesso em: 05 jun. 2024.

TEPEDINO, Gustavo. **Novos princípios contratuais e a teoria da confiança: a exegese da cláusula to
thebest knowledge of the sellers**. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5600369/mod_resource/content/1/Novos%20Princ%C3%ADpios%20Contratuais%20e%20Teoria%20da%20Confian%C3%A7a%20a%20exegese%20da%20cl%C3%A1usula%20to%20the%20best%20knowledge%20of%20the%20sellers%20-%20Gustavo%20Tepedino%20.pdf. Acesso em: 28 jun. 2021.

TOLEDO, Mônica. Hackers invadem sistema do Hospital de Câncer de Barretos e pedem resgate. **Folha de São Paulo**. 2017. Disponível em: https://www1.folha.uol.com.br/cotidiano/2017/06/1896638-hackers-invadem-sistema-do-hospital-de-cancer-de-barretos-e-pedem-resgate.shtml. Acesso em: 26 dez. 2023.

TRIBUNAL REGIONAL DO TRABALHO (3ª Região). **Trabalhador dispensado de forma discriminatória após ser diagnosticado com HIV será reintegrado**. Minas Gerais, 19 out. 2021. Seção de Imprensa. Disponível em: https://portal.trt3.jus.br/internet/conheca-o-trt/comunicacao/noticias-juridicas/trabalhador-dispensado-de-forma-discriminatoria-apos-ser-diagnosticado-com-hiv-sera-reintegrado. Acesso em: 15 nov. 2023.

TRIPWIRE. **Why Hackers Are After The Healthcare Industry**. 2015. Disponível em: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/why-anthem-why-now/. Acesso em: 26 dez. 2023.

TUNGGAL. Allan Toh. What is a Data Leak? Stop Giving Cybercriminals Free Access. **UpGuard,** 2023. Disponível em: https://www.upguard.com/blog/data-leak. Acesso em: 26 dez. 2023.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados **(Regulamento Geral sobre a Proteção de Dados).** Jornal Oficial da União Europeia. L 119/1, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 29 maio 2024.

VIOLA, Marcelo; TEFFÉ, Carolina. Tratamento De Dados Pessoais Na LGPD: Estudo Sobre as Bases Legais Dos Artigos 7.º E 11. *In:* DONEDA, D. et al. (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. cap. 6.

WISKY, Daniel. SOLID. Princípio da Responsabilidade Única. **Blog Daniel Wisky**, 2023. Disponível em: https://danielwisky.com.br/2023-08-05-principio-responsabilidade-unica/#:~:text=O%20Princ%C3%ADpio%20da%20Responsabilidade%20%C3%9Anica,e%20a%20extensibilidade%20do%20c%C3%B3digo. Acesso em: 08 jan. 2024.

ZISMAN, Carlos Roberto. A dignidade da pessoa humana como princípio universal. **Revista de Direito Constitucional e Internacional**. Vol. 96, jul. 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDConsInter_n.96.06.PDF. Acesso em: 26 jun. 2021.

SOLOVE, Daniel. Data is what data does: regulating use, harm, and risk instead of sensitive data. **Northwestern University Law** *Review*, v. 118, jan. 2023, p. 35-36. Disponível em: https://ssrn.com/abstract=4322198. Acesso em: 11 nov. 2023.