PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD

BIANCA RAFAELA LUIZA AMORIM BULZICO

O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NO ÂMBITO DOS SISTEMAS INTERROPERÁVEIS DE SAÚDE: UMA ANÁLISE NO CAMPO DA SEGURANÇA DA INFORMAÇÃO E DA PRIVACIDADE

CURITIBA
2022

BIANCA RAFAELA LUIZA AMORIM BULZICO

O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NO ÂMBITO DOS SISTEMAS INTERROPERÁVEIS DE SAÚDE: UMA ANÁLISE NO CAMPO DA SEGURANÇA DA INFORMAÇÃO E DA PRIVACIDADE

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Socioambiental e Sustentabilidade e na linha de pesquisa em Estado, Sociedades, Povos e Meio Ambiente, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de mestre.

Orientador: Profª. Drª. Cinthia Obladen de Almendra Freitas

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Pamela Travassos de Freitas CRB/9 1960

Bulzico, Bianca Rafaela Luiza Amorim
B941t 2022 O tratamento de dados pessoais sensíveis no âmbito dos sistemas interroperáveis de saúde : uma análise no campo da segurança da informação e da privacidade / Bianca Rafaela Luiza Amorim Bulzico ; orientador: Cinthia Obladen de Almendra Freitas. – 2022.
115 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2022
Bibliografia: f. 102-115

1. Direito privado. 2. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 3. Direito à privacidade. 4. Proteção de dados. 5. Tecnologia da Informação - Medidas de segurança. I. Gonçalves, Oksandro Osdival. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título.

Doris 3. ed. – 342

Pontifícia Universidade Católica do Paraná
Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação
Diretoria de Pós-Graduação stricto sensu

ATA DE DEFESA DE DISSERTAÇÃO N.º 656

Programa de Pós-Graduação em Direito - Mestrado
Área de Concentração: Direito Socioambiental e Sustentabilidade
Linha de Pesquisa: Estado, Sociedades e Meio Ambiente

Aos 17/03/2022 14:00, na sala/auditório PUCPR da PUCPR, reuniu-se em ato público a Banca Examinadora de dissertação do(a) mestrando(a) ***Bianca Rafaela Luiza Amorim Bulzico***, orientado(a) pelo(a) Professor(a) Doutor(a) ***CINTHIA OBLADEN DE ALMENDRA FREITAS*** e composta pelos pesquisadores examinadores abaixo relacionados, ocasião em que se realizou a arguição da dissertação intitulada ***"O Tratamento de Dados Pessoais Sensíveis no âmbito dos Sistemas Interoperáveis de Saúde: uma análise no campo da segurança da informação e da privacidade";*** . Concluídos os trabalhos, os membros da Banca Examinadora consideram a dissertação:

(X) Aprovada, ( ) Aprovada com restrições, ( ) Não Aprovada.

Observações:

Nada mais havendo a tratar, a sessão foi encerrada às 17 horas e 55 minutos, dela sendo lavrada a presente ata, que segue assinada pelos membros da Banca Examinadora e pelo(a) Candidato(a).

O(A) candidato(a) está ciente que a concessão do referido título está condicionada à: (i) satisfação dos requisitos solicitados pela Banca Examinadora.; (ii) entrega da dissertação em conformidade com as normas exigidas pelo Programa; (iii) atendimento aos requisito de publicação estabelecido nas normas do Programa e (iv) entrega da documentação necessário para elaboração do Diploma. A Banca Examinadora determina um **prazo máximo de** 30 **dias**, considerando os prazos máximos definidos no Regulamento do Programa, para o cumprimento dos requisitos (desconsiderar caso reprovado), sob pena de, não o fazendo, ser desvinculado do Programa sem o Título de Mestre.

Profa Dra : CINTHIA OBLADEN DE ALMENDRA FREITAS Orientadora	nota: 9,5	(X) Aprovada ( ) Aprovada com restrições ( ) Não aprovada
Prof Doutor : ALTAIR OLIVO SANTIN Membro Interno ALTAIR OLIVO SANTIN:65696611915 Assinado de forma digital por ALTAIR OLIVO SANTIN:65696611915 DN: c=BR, o=ICP-Brasil, ou=presencial, ou=34028316000103, ou=Secretaria da Receita Federal do Brasil - RFB, ou=ARCORREIOS, ou=RFB e-CPF A3, cn=ALTAIR OLIVO SANTIN:65696611915 Dados: 2022.04.07 19:30:12 -03'00'	nota: 9,5	(X) Aprovada ( ) Aprovada com restrições ( ) Não aprovada
Profa Doutor : Claudia Maria Barbosa Membro Interno gov.br Documento assinado digitalmente CLAUDIA MARIA BARBOSA Data: 07/04/2022 16:38:20-0300 Verifique em https://verificador.iti.br	nota: 9,5	(X) Aprovada ( ) Aprovada com restrições ( ) Não aprovada
Prof(a) Doutor : Vinícius Borges Fortes Membro Externo vinculado(a) a IMED-RS	nota: 9,5	(X) Aprovada ( ) Aprovada com restrições ( ) Não aprovada

BIANCA RAFAELA LUIZA AMORIM BULZICO Assinado de forma digital por BIANCA RAFAELA LUIZA AMORIM BULZICO Dados: 2022.04.04 15:25:48 -03'00'	
Assinatura Candidata	Assinatura Coordenador do Programa

CURITIBA

2022

BIANCA RAFAELA LUIZA AMORIM BULZICO

O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NO ÂMBITO DOS SISTEMAS INTERROPERÁVEIS DE SAÚDE: UMA ANÁLISE NO CAMPO DA SEGURANÇA DA INFORMAÇÃO E DA PRIVACIDADE

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Socioambiental e Sustentabilidade e na linha de pesquisa em Estado, Sociedades, Povos e Meio Ambiente, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de mestre.

COMISSÃO EXAMINADORA

_____

Profª. Drª. Cinthia Obladen de Almendra Freitas

Pontifícia Universidade Católica do Paraná (PUCPR) – Orientadora

_____

Profª. Drª. Claudia Maria Barbosa

Pontifícia Universidade Católica do Paraná (PUCPR) – Avaliadora

_____

Prof. Dr. Vinícius Borges Fortes

Faculdade IMED – Avaliador

_____

Prof. Dr. Altair Olivo Santin

Pontifícia Universidade Católica do Paraná (PUCPR) – Avaliador

Curitiba, 17 de março de 2022.

*Aos meus pais, **Edna e Braulio**, por sempre acreditarem em mim e por terem abdicado tanto em suas vidas em prol das realizações e felicidade de suas filhas.*

*À minha irmã, **Bettina**, ícone de inspiração, e, toda à família, pela preocupação e carinho incondicional.*

*Ao meu noivo, **Tiago**, pela compreensão, cuidado e incentivo diário.*

Sem vocês nada disso teria sentido.

AGRADECIMENTOS

A **Deus**, pela dádiva da vida e por me permitir realizar tantos sonhos nesta existência. Obrigada por me permitir errar, aprender e crescer, por Sua eterna compreensão e tolerância, por Seu infinito amor, pela Sua voz “invisível” que não me permitiu desistir e principalmente por ter me dado uma família tão especial, enfim, obrigado por tudo. Lembro de todos os dias que orei para realizar tudo o que vivo hoje!

A **Profª. Cinthia**, pela orientação, dedicação, profissionalismo e atenção tão importantes em todas as etapas. Tantas vezes que conversamos, embora pouquíssimas vezes pessoalmente, suas palavras transmitiam todo o incentivo e ânimo que eu precisava para continuar perseguindo o objetivo do trabalho. Sua admirável aptidão profissional, me fez descobrir um carinho especial pela pesquisa e pela tecnologia. Obrigado por acreditar em mim. Tenho certeza que não chegaria neste ponto sem o seu apoio.

Aos membros da banca examinadora, **Profª Claudia Maria Barbosa**, **Prof. Vinícius Borges Fortes** e **Prof. Altair Olivo Santin**, que tão gentilmente aceitaram participar e colaborar com esta dissertação.

A todos **amigos e amigas do PPGD da PUCPR**, em especial ao *“Time Cinthia”*, obrigada por todo o carinho, apoio e amizade demonstrados.

Ao **Programa de Pós-Graduação em Direito da PUCPR**, minha gratidão aos professores, colegas, funcionários, especialmente às secretárias, dentre outros inomináveis que, direta ou indiretamente, contribuíram neste percurso tão valoroso da construção do conhecimento e aprimoramento da minha formação.

A **Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)** junto ao **Programa de Cooperação Acadêmica em Segurança Pública e Ciências Forenses (PROCAD/SPCF)**, agradeço pela bolsa de estudos concedida para compor o Projeto SiCReT II (Sistema de Cruzamento de Registros Telefônicos), sob a coordenação da Prof.ª Drª. Cinthia Obladen de Almendra Freitas, o qual permitiu ampliar as pesquisas e conciliar com a escrita desta dissertação.

Por fim, a todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação, o meu sincero agradecimento.

“A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém pensou sobre aquilo que todo mundo vê.”

(Arthur Schopenhauer)

RESUMO

No setor de saúde o uso de ferramentas inovadoras e tecnológicas facilitam a assistência ao paciente no cotidiano e favorecem um diagnóstico mais assertivo. Uma das ferramentas utilizadas é a padronização e a troca de dados entre interfaces operacionais que integram inúmeras informações a respeito do estado de saúde do paciente. A tecnologia utilizada para o compartilhamento desses dados, é a interoperabilidade, entretanto, diversas são as ferramentas de segurança da informação aplicáveis a estes sistemas. Logo, indaga-se: os mecanismos de segurança da informação utilizados pela saúde são suficientes para garantir a integridade do dado e a privacidade do titular? Para verificar as hipóteses de vulnerabilidade dos sistemas na troca de dados, o objetivo geral do trabalho se concentrou em desenvolver a revisão de legislações nacionais que abrigam a proteção à privacidade e intimidade; aprofundar a arquitetura dos sistemas computacionais padrões utilizados em saúde, em especial, no padrão de Troca de Informações na Saúde Suplementar (TISS). Em seguida, os objetivos específicos se desenvolveram para: demonstrar o funcionamento e finalidade dos padrões computacionais comumente utilizados pela saúde; identificar os *assets* de segurança da informação entre o padrão TISS e HL7; aproximar as vulnerabilidades computacionais da probabilidade de dano à privacidade do titular; rever as previsões legais que orientam a implementação de uma segurança da informação adequada. Dividido em três capítulos, o primeiro se preocupou em construir bases teóricas para fundamentar o desenvolvimento do trabalho; no capítulo seguinte, demonstrou a dinâmica do compartilhamento de dados no TISS e indicar os *gaps* de segurança que a interface possui; e no último capítulo, por fim, com base nas previsões da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709 de 2018 (LGPD), propôs alterações dos elementos frágeis de segurança identificados. Portanto, a hipótese da pesquisa foi confirmada, uma vez que a segurança computacional do padrão de troca de dados analisado, o dado pode sofrer alterações comprometendo sua integridade, além de incorrer em risco à privacidade do titular. Para atingir o resultado, o trabalho utilizou como metodologia a pesquisa bibliográfica no aprofundamento dos conceitos e desenvolvimento dos capítulos que, por meio de método hipotético-dedutivo, favoreceu a identificação de falhas de segurança do sistema TISS utilizado na comunicação de planos de assistência à saúde suplementar. Concluiu-se que os direitos individuais à privacidade e intimidade podem sofrer ameaça diante da probabilidade de exposição desautorizada de dados dos titulares quando compartilhados pelo TISS com outros sistemas sem as devidas medidas de segurança, e, portanto, comprometendo o sigilo dos dados e informações e a ruptura dos deveres legais.

Palavras-chave: Novas Tecnologias. Estado. Proteção de dados. Dados sensíveis. Segurança da Informação.

ABSTRACT

In the health sector, the use of innovative and technological tools favor to patient care in everyday life and favor a more assertive diagnosis. One of the tools used is the standardization and exchange of data between operational interfaces that integrate numerous information about the patient's health status. The technology used to share this data is interoperability, however, there are several information security tools applicable to these systems. Therefore, the question is: are the information security mechanisms used by healthcare sufficient to guarantee data integrity and the privacy of the data subject? To verify the hypotheses of vulnerability of systems in the exchange of data, the general objective of the work focused on developing the review of national legislation that shelters the protection of privacy and intimacy; to deepen the architecture of standard computer systems used in health, especially in the Supplementary Health Information Exchange (TISS) standard. Then, specific objectives were developed to: demonstrate the functioning and purpose of computational standards commonly used by health; identify information security assets between the TISS and HL7 standard; approximate computing vulnerabilities to the probability of damage to the data subject's privacy; review the legal provisions that guide the implementation of adequate information security. Divided into three chapters, the first was concerned with building theoretical bases to support the development of the work; in the following chapter, he demonstrated the dynamics of data sharing in TISS and indicated the security gaps that the interface has; and in the last chapter, finally, based on the provisions of the General Law for the Protection of Personal Data - Law No. 13.709 of 2018 (LGPD), it proposed changes to the identified fragile security elements. Therefore, the research hypothesis is confirmed, since the computational security of the data exchange pattern analyzed, the data can undergo changes compromising its integrity, in addition to incurring a risk to the privacy of the data subject. To achieve the result, the work used as a methodology the bibliographic research in the deepening of the concepts and development of the chapters that, through a hypothetical-deductive method, favored the identification of security flaws of the TISS system used in the communication of health care plans additional. It was concluded that individual rights to privacy and intimacy may be threatened by the likelihood of unauthorized exposure of data subjects when shared by TISS with other systems without proper security measures, and therefore compromising the confidentiality of data and information and breach of legal duties.

Keywords: New technologies. State. Data protection. Sensitive data. Information Security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANS	Agência Nacional de Saúde Suplementar
CFM	Conselho Federal de Medicina
HL7	*Hight Level Seven*
ISO	*International Organization for Standardization*
LAI	Lei de Acesso a Informação
LGPD	Lei Geral de Proteção de Dados
PEP	Protocolo Eletrônico do Paciente
RES	Registro Eletrônico em Saúde
SGSI	Sistema de Gerenciamento de Segurança da Informação
SI	Sistema da Informação
TISS	Troca de Informação na Saúde Suplementar
TUSS	Terminologia Unificada na Saúde Suplementar

SUMÁRIO

INTRODUÇÃO

Desde o seu surgimento, a tecnologia influencia o comportamento da sociedade, pois é implementada como ferramenta auxiliar na transformação em diferentes áreas de atuação do cotidiano.

O fenômeno da globalização que ao mesmo tempo proporciona o acesso facilitado à rede mundial de computadores e colabora para o crescimento do número de usuários ativos na *web;* em contrapartida, despeja a todo instante dados pessoais desses usuários na rede. Atrelados a estes elementos, a exposição do usuário colocou em risco direitos constitucionalmente previstos e raramente respeitados nesse contexto: a intimidade e a privacidade, seja por parte do Estado, das empresas ou até mesmo por parte dos próprios usuários.

O volumoso número de dados disponibilizados na *web*, trouxe advertência ao uso indiscriminado de novas tecnologias, especialmente de informação e comunicação. Nesse aspecto, as afirmações de referência trazidas por Stefano Rodotá (2008) confirmam que a disponibilidade de meios tecnológicos não legitima todas as suas formas de utilização. Pelo contrário, o uso deve estar pautado em valores dignos para que estes se sobreponham a simples massificação da informação freando a recorrente transformação de dados em mercadoria.

Nesse viés voltado à proteção da personalidade jurídica dos titulares de dados pessoais, entrou em vigor, em setembro de 2020, a Lei Geral de Proteção de Dados Pessoais nº 13.709 de 2018 (LGPD) que reforça a tutela até então exercida pela Lei nº 12.965 de 2014, conhecida como Marco Civil da Internet, incluindo respaldo jurídico não apenas em meio digital mas também físico.

O legislador foi além, e inseriu uma nova categoria de proteção ao tratamento de dados pessoais, quais seja a categoria especial de “dados pessoais sensíveis”, aqueles que, sob a assunção de Bruno Bioni (2019) podem gerar discriminação, pois estão relacionados com a personalidade do indivíduo e suas escolhas pessoais, uma vez que fazem remissão à orientação sexual, religiosa, racial, estado de saúde ou filiação sindical do titular desses dados (art. 5º, inciso II, LGPD).

Essa categoria de dados pessoais provocou a necessidade de cumprir com requisitos mínimos para o tratamento legal, dentre eles a coleta com o consentimento do titular de dados.

Os dados coletados por hospitais e clínicas de atendimento à saúde, em sua maioria, são dados pessoais sensíveis e o consentimento do paciente inclina-se à necessidade do atendimento, reservados aos aspectos éticos que compreendem a atuação profissional médica na guarda e sigilo dessas informações, reforçados inclusive pelo Código de Ética Médica aprovado pela Resolução nº2.217 de setembro de 2018 (BRASIL, 2018).

Autorizado pelo texto da Lei nº 13.787 de 2018 (BRASIL, 2018), o Prontuário Eletrônico do Paciente (PEP) passou a ser disponibilizado para agregar e resguardar os dados e informações de saúde do paciente, incorporando ao Registro Eletrônico de Saúde (RES) (BRASIL, 2018), favorecendo a assistência à saúde do paciente pela facilidade no acesso do conteúdo pelos profissionais da categoria médica.

Nesse contexto, invoca a problemática da pesquisa: os *assets* de segurança da informação dos sistemas computacionais utilizados para a saúde são suficientes para garantir a integridade do dado e a privacidade do titular?

Em busca da resposta ao questionamento evocaram-se duas hipóteses: a primeira sobre a verificação de vulnerabilidade na troca de dado; e a segunda, direcionada ao rigor da segurança da informação adotada pela arquitetura do sistema computacional do Padrão TISS.

Segundo dados da ANS (Agência Nacional de Saúde), no último ano de 2021 o número de beneficiários de planos de saúde somou quase 49 milhões de pessoas. Dessa forma, o resultado dessa pesquisa é direcionado ao número de beneficiários que possuem seus dados registrados em bases de dados de planos de saúde privados, cuja a comunicação entre sistemas é feita através da interoperabilidade, podendo estar sob vulnerabilidades na troca dessas informações.

Logo, o objetivo geral proposto se volta a em desenvolver a revisão de legislações nacionais que abrigam a proteção de dados e os direitos da personalidade do titular, além das Resoluções Normativas instituídas pela própria Agência Nacional de Saúde Suplementar (ANS).

Inclusive, a tecnologia interoperável utilizada para a comunicação entre sistemas híbridos, com diferentes interfaces, foi autorizada pelo Ministério da Saúde com a entrada em vigor da Portaria nº2.073 de 2011 (BRASIL, 2011) que regulamentou o uso dessa tecnologia em âmbito público e privado. Ainda, instituiu o "*Catálogo de Padrões de Interoperabilidade de Informações e Sistemas de Saúde (CPIISS)"* que cita a implementação de alguns padrões facilitadores para persecução da assistência

ao paciente e que são frequentemente utilizados pelos profissionais de saúde, sejam eles: OpenEHR, HL7, SNOMED-CT, TISS, HL7CDA, DICON, LOINC, ISBT128, ISO 136062, IHE-PIX, CID, CIAP-2, TUSS e CBHPM.

Já os objetivos específicos se concentram aprofundar o funcionamento e finalidade desses padrões computacionais mencionados; identificar os *assets* de segurança da informação especialmente do Padrão TISS e HL7; aproximar as vulnerabilidades computacionais da probabilidade de dano à privacidade do titular; e, por fim, rever as previsões legais que orientam a implementação de uma segurança da informação adequada.

O trabalho se apresenta dividido em três capítulos, do qual o primeiro se preocupou na construção de bases teóricas para embasar todo o desenvolvimento do trabalho; no capítulo seguinte, demonstrou a dinâmica do compartilhamento de dados no TISS com indicação aos *gaps* de segurança que a interface possui; e, por fim, o último capítulo confirmou a existência de elementos de segurança da informação fragilizados e que podem conferir risco ao titular, de acordo com a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709 de 2018 (LGPD).

Com a atenção voltada aos padrões TISS e HL7, verifica que o desenvolvimento do formato do padrão nacional (TISS) utilizou como base a arquitetura do internacional (HL7) que, além de norma, desenvolve outras normas e especificações, protocolos ou padrões que devem ser utilizados na troca de dados clínicos e administrativos em Sistemas da Informação (SI).

Mesmo que o Padrão TISS seja utilizado como um sistema padrão com finalidade primária de troca de informações de cunho “gerencial” utilizado por empresas privadas de assistência à saúde, por outro lado, sua estrutura possibilita – em alguns momentos – que o titular possa ser identificado, a ponto de converter um dado pessoal comum em um dado pessoal sensível.

Ademais, diante das exigências de boas práticas previstas pela LGPD, o presente trabalho desenvolve como objetivo geral a retomada de direitos individuais como proteção constitucional, quando dados sensíveis são cedidos por seus titulares para complementar a base de dados do sistema operacional TISS que, ao comunicar-se com outros sistemas pode comprometer o sigilo do conteúdo devido a sua vulnerável arquitetura de segurança.

Encaminha-se, portanto, ao desenvolvimento dos objetivos específicos para desenvolver os conceitos e fundamentos que embasam o trabalho e, posteriormente,

analisar o funcionamento operacional do Padrão TISS e as fragilidades existentes na sua constituição que podem oferecer risco a vida privada do beneficiário/titular de dados.

A pesquisa, ainda, envolve o conhecimento detalhado da arquitetura de padrões, aprofundamento em técnicas operacionais de transporte de dados, mecanismos de segurança, Segurança da Informação (SI); também utiliza as alterações e inovações trazidas pela Lei Geral de Proteção de Dados Pessoais na busca por reforço a defesa da privacidade e a intimidade do titular, especificamente do paciente frente ao sistema de saúde brasileiro.

A vinculação da pesquisa na área de concentração de “Direito Socioambiental e Sustentabilidade” e o envolvimento com a linha de pesquisa em “Estado, Sociedades, Povos e Meio Ambiente” se dá por meio de contribuição que visa auxiliar a retomada da proteção aos direitos individuais previstos pela Constituição Federal que perdem evidência quando equiparados ao surgimento de novas ferramentas tecnológicas.

Para a proposição final do trabalho, verificou-se que para afirmar a existência de garantia na proteção do indivíduo diante do compartilhamento de dados entre sistemas interoperáveis, fez-se necessário verificar os *assets* de segurança do sistema operacional que realiza essa dinâmica. O TISS, utilizado como elemento de análise, demonstrou fragilidade em sua arquitetura no que tange à segurança, capaz de expor os dados compartilhados e identificar o titular das informações.

Para atingir o resultado, fez-se uso de pesquisa qualitativa, argumentando os resultados do estudo por meio de análises e percepções tanto do cenário jurídico, quanto da área de Segurança da Informação (SI). As premissas e hipóteses de os sistemas operacionais apresentarem vulnerabilidades com a possibilidade de exposição do titular, foram construídas pelo uso do método hipotético-dedutivo.

Sem pretensão de esgotar o tema, a contribuição da pesquisa é reafirmar a importância da inviolabilidade de direitos da personalidade constitucionalmente previstos nos diplomas legais, além de romper com a informalidade no compartilhamento de dados pelo TISS, uma vez que o ambiente de compartilhamento dessas informações pode ser corrompido gerando danos aos titulares.

CAPÍTULO I – CONCEITOS E FUNDAMENTOS SOBRE PROTEÇÃO DE DADOS E TECNOLOGIA UTILIZADOS NOS SISTEMAS INTEROPERÁVEIS DA SAÚDE

Neste primeiro capítulo foram apresentados os fundamentos e definições essenciais que embasam o desenvolvimento do tema para que à frente possa ser tratado sobre os efeitos da tecnologia na área da saúde, e como os dados pessoais sensíveis afetos a essa dinâmica, de exposição e interoperabilidade, devem ser resguardados de acordo com a legislação brasileira.

1.1. Privacidade e proteção de dados na saúde

No Brasil, assim como em diversos outros Estados, a privacidade é assegurada e tutelada como um direito humano fundamental. Tentar definir privacidade pode levar a uma conceituação demasiadamente ampla ou estrita, impedindo assim que problemas ligados à sua violação possam ser analisados, prevenidos ou remediados (CANCELIER, 2017).

Danilo Doneda (2019) registra a ausência de um conceito que ancore em definitivo o que se entende pelo termo “privacidade”, indicando ser este um problema não apenas presente na doutrina nacional brasileira, mas também internacional, sugerindo, assim, um regresso às bases históricas.

Narra-se aqui a emblemática publicação de Louis Brandeis e Samuel Warren, em 1890, do artigo intitulado *“The Right to Privacy*”, na *Harvard Law Review,* referência indispensável e marco nas discussões sobre a temática de privacidade.

Os autores, entendiam a privacidade como um direito de “ser deixado só” – *the right let to be alone* – ou à “não intrusão”, passando a revelar-se como um importante instrumento para garantir o próprio exercício da liberdade (WARREN; BRANDEIS, 1890).

Originalmente, o material escrito discorre sobre a ameaça potencial à vida privada dos indivíduos pelas mudanças tecnológicas da época, em especial àquelas trazidas pelas novas formas de obtenção à informação (fotos, vídeos, telefonia, etc.), e de qual forma o *Common Law* poderia se desenvolver no sentido de salvaguardar o interesse do que se conhecia como privacidade (WARREN; BRANDEIS, 1890).

Diferente do que afirma Kalline Eler (2016), a identificação da privacidade por Warren e Brandeis (1890) se desprende da característica antecedente ao direito de “ser deixado só” vinculado ao sistema patriarcal com seu sentido voltado

essencialmente em alimentar o isolamento e a reclusão (DONEDA, 2019), ultrapassando, portanto, esses limites e direcionando a preocupação da intimidade do indivíduo frente aos novos fatos sociais e às possibilidades invasivas dos meios de comunicação que levavam à público as informações, essencialmente à imprensa (BOFF; FORTES; FREITAS, 2018).

O encargo da mídia em levar informação à sociedade mediante uma coleção de materiais audiovisuais, conduziu Warren e Brandeis (1890) a outorgar o conceito de privacidade àquele em que toda a pessoa possui plena disponibilidade para decidir em qual medida seus pensamentos, sentimentos e emoções podem ser comunicados a coletividade. Neste ponto, Boff, Fortes e Freitas (2018) entendem que o direito à privacidade passou a integrar o conjunto de direitos de liberdade e de propriedade.

Por meio de uma análise histórica dos fundamentos que levaram os autores Warren e Brandeis (1890) na construção do artigo, Saldanã (2012) confirma que o direito de liberdade e intimidade, originalmente denominado "*right to privacy*"[1], mesmo ampliado o leque de privilégios civis, seria incapaz de confirmar a proteção definitiva à privacidade; ao mesmo passo que o direito à propriedade que garante ao indivíduo a posse, seja ela tangível ou intangível, não alcança a mesma garantia aos dados pessoais que podem ser alvo de publicação e exposição.

O direito à privacidade, portanto, garante ao indivíduo o poder de dispor e decidir a respeito de seus interesses imateriais, configurando-se como um direito propriamente subjetivo e de caráter autônomo (BOFF; FORTES; FREITAS, 2018, p. 65). Cabe, portanto, ao indivíduo, o dever de decisão a respeito da publicização ou não de dados pessoais considerando os aspectos de privacidade, seja ela no âmbito privado – restrita ao indivíduo – ou público – com base no legítimo reconhecimento pela sociedade.

É a partir deste ponto que se revisita as características de isolamento para reconfigurar a terminologia, com o fim de evitar a ocorrência de violações à vida privada. Essa violação pode ocorrer tanto por ato lícito, quando o indivíduo voluntariamente repassar dados destinados à uma finalidade inicial, entretanto, sem autorização, acabam sendo utilizados para finalidade diversa; como ilícito, quando

---

[1] Tradução livre: direito de privacidade

dados pessoais de caráter sigiloso são coletadas clandestinamente com a intenção de torná-los público (BOFF; FORTES; FREITAS, 2018).

No presente contexto social, os dados se tornaram elementos indispensáveis para a vida civil, política, econômica, educacional, financeira, etc., de modo que a sociedade contemporânea e informacional convive com um volume infindável de dados coletados e presencia o descontrole sobre seus dados frente à multiplicidade de plataformas, redes sociais e sistemas operacionais.

Nas palavras de Danilo Doneda (2019, p. 137), o dado pessoal é aquele ligado estritamente ao estado e condição do indivíduo e que, portanto, apresenta 02 (dois) fatores principais: a eficiência e o controle, articulados por uma série de interesses de caráter público ou privado.

O conglomerado de dados, alude ao significado de “informação” que pressupõe um processo de interpretação (DONEDA, 2019). Por si só, a informação possui caráter de “comunicar”, através de diversos meios disponíveis.

No entanto, Doneda (2019, p.136) afirma que a informação carrega historicamente “maior desenvoltura de sua manipulação, desde sua coleta e tratamento, até sua comunicação” e, especialmente, isso se comprova com a utilização de meios de comunicação inovadores e tecnológicos para a propagação.

Considerando a alta complexidade e o alto custo em levar a informação ao conhecimento público, o Estado ocupou larga vantagem na utilização e na favorável manipulação de dados pessoais. Esse modelo de gestão por parte do Estado deu forma ao “*welfare state*”[2] definido como um modelo de Estado assistencialista e intervencionista fundado nos direitos sociais e no bem-estar dos cidadãos (GOMES, 2006).

Sem dúvidas essa dinâmica fortaleceu as diversas formas de controle social que podem ser desempenhadas pelo Estado e que seriam disponibilizadas com maior potencialidade de informações sobre indivíduos (DONEDA, 2019). A sensação de “proteção”, na verdade nada mais seria do que controle pelo ente público de dados e, posterior, informações congregadas de todos os cidadãos.

---

[2] Tradução livre: estado de bem-estar

Essa atividade, até então predominante aos entes públicos, passou a ganhar espaço pelas entidades privadas (DONEDA,2019) com o desenvolvimento de tecnologias inovadoras que facilitaram a coleta e o processamento de dados.

A ampla utilização de dados pessoais para as mais variadas finalidades, seja identificação, classificação, autorização e tantas outras, permite com que esses dados cumpram com a razão da emersão na denominada Sociedade da Informação.

Como bem define Castells (2000, p. 25) a expressão “Sociedade da Informação” passou a ser utilizada, nos últimos anos desse século, como substituto ao complexo conceito de “sociedade pós-industrial”. Fato é que neste ponto a informação passou a ser um insumo de baixo custo para aquisição pelas organizações administrativas, favorecidas pelos avanços tecnológicos na microeletrônica e nas telecomunicações.

De certa forma, os fatores: liberdade e propriedade, até então voltados para a autonomia do indivíduo em dispor de informações pessoais, não contavam, propriamente, com a entrada avassaladora das Tecnologias de Informação e Comunicação (TICs).

Atualmente, a denominada Sociedade da Informação está fundamentalmente ligada à utilização das TICs, conhecidas como computador, tablet, telefones móveis, televisão interativa, redes de comutadores, estruturas sem fio (*wireless*) e, é claro, o acesso à Internet (RAMINELLI; RODERGHERI, 2016).

Assim, considerando o interesse por parte da população em adquirir objetos tecnológicos para comunicação e realização de outras atividades no dia a dia, se fez necessário redefinir estratégias legais para aumentar o grau de proteção ao direito de privacidade.

Ao tratar de proteção legal à privacidade, elenca-se imediatamente os direitos fundamentais previstos na Constituição Federal Brasileira que compreendem além da preservação à vida privada, a intimidade da pessoa, a inviolabilidade da correspondência, do domicílio e das comunicações, em consonância com o fundamento do inciso X, do artigo 5º, da CF (BRASIL, 1988). Ainda, há previsão alocada no Código Civil Brasileiro (BRASIL, 2002) que também ampara o direito à privacidade, este intimamente ligado ao direito à intimidade e ao princípio da dignidade da pessoa humana.

A privacidade foi ganhando importância e reconhecimento jurídico tanto no cenário nacional quanto internacional (HIRATA, 2017), valendo citar,

exemplificativamente, documentos expressivos dos quais o Brasil é signatário, como a Convenção Americana dos Direitos e Deveres do Homem, datada de 1948 , cujo o artigo V estatui que “toda pessoa tem direito à proteção a lei contra s ataques abusivos à sua honra à sua reputação e à sua vida particular e familiar” (DECLARAÇÃO AMERICANA, 1948), e a Declaração Universal dos Direitos Humanos, do mesmo ano, que no artigo 12 expressa que “ninguém será sujeito a interferência em sua vida privada, em sua família, em seu lar, sua correspondência, em a ataque à sua honra e reputação.” (DECLARAÇÃO UNIVERSAL, 1948).

A amplificação do acesso à Internet como um espaço aberto propício para a difusão das mais variadas temáticas, independentemente de barreiras temporais ou territoriais, permitiu que pessoas consumissem, produzissem e distribuíssem informações sob qualquer formato em tempo real e para qualquer lugar do mundo (LEMOS; LÉVY, 2010).

Do produto dessa alta demanda, emergiu a preocupação com o tratamento de dados pessoais pois estaria dispondo diretamente a intimidade e vida privada dos indivíduos (RAMINELLI; RODERGHERI, 2016), fato que vem inspirando a edição de leis e regulamentações específicas sobre a matéria em nível global.

Decorrente do aspecto positivo do direito à intimidade, necessário se faz mencionar a autodeterminação informativa como um direito humano fundamental com conteúdo próprio, que não se limita em garantir a vida privada e a intimidade (CASTRO, 2013); diferentemente da tese negativa, que defende a autodeterminação informativa como uma faculdade de dispor dados pessoais guiada pelo instituto da autonomia à conduta, ou seja, como um complemento do direito da personalidade (LIMBERGER, 2007).

Pelo viés traçado por Catarina Sarmento e Castro (2013), os direitos fundamentais conflitam com a segurança, uma vez que a difusão da Internet imprimiu um novo significado à intimidade e, por consequência, à privacidade. Portanto, é nesse ponto que a doutrina salienta a necessidade de inserir no rol de direitos fundamentais a autodeterminação informativa, visando somar aos direitos e não os contrapor (CASTRO, 2013).

Interessante notar que a necessidade de proteção jurídica do cidadão com relação aos dados pessoais origina-se da constatação de que esses dados que circulam na *web* possuem conteúdo com valor econômico. Maria Eduarda Gonçalves (2003) afirma que, com o fenômeno da globalização, o direito à informação vem sendo

tratado como mercadoria sob o qual incidem interesses econômicos, reduzindo a importância do indivíduo como titular daquela informação.

Diante dessa realidade, Rodotà (2008) adverte que a simples disponibilidade de uma tecnologia não legitima todas as suas formas de utilização, pelo contrário, a utilização deve ser avaliada com base em valores dignos para que se sobreponham a simples massificação da informação e de sua transformação em mercadoria.

Em se tratando do exercício digno de direitos voltados à liberdade pessoal, a integridade e a dignidade, não se pode aceitar que a necessidade de segurança ou o objetivo voltado à eficiência se sobreponham acima de quaisquer outras considerações. Eleva a necessidade de elencar a proteção legal conferida aos dados e informações pessoais coletados indiscriminadamente.

No Brasil, a Lei nº 12.965 de 2014, conhecida como Marco Civil da Internet propõe estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil (BRASIL, 2014). Mais recentemente, em 14 de agosto de 2018, foi promulgada a Lei 13.709/2018, a Lei Geral de Proteção e Dados Pessoais (LGPD), responsável por aprofundar a regulamentação de questões relativas ao tratamento de dados pessoais no cenário nacional (BRASIL, 2018).

Os impactos da LGPD são expressivos, tanto no aspecto de tutela à privacidade e proteção de dados pessoais de seus respectivos titulares, quanto, naturalmente, para a atividade empresarial e administração pública, considerando que a LGPD impõe uma série de diretrizes para que o tratamento de dados seja realizado de forma lícita, com o consentimento do titular (BRASIL, 2018).

A superproteção de dados pessoais componentes do núcleo duro dos direitos fundamentais, não advém apenas da necessidade de sigilo, mas principalmente, da necessidade de impedir discriminações entre cidadãos e a elaboração de perfis individuais que poderiam resultar em tratamentos desiguais ou discriminatórios.

Dessa forma, além da legislação formal, a proteção de dados pessoais também alcança princípios (RODOTÁ, 2008) que devem ser levados em consideração, quais sejam:

a) princípio da correção: garantia dada ao indivíduo para a correção adequada de seus dados a qualquer tempo;

b) princípio da exatidão das informações;

c) princípio da finalidade: toda a utilização de dados pessoais deve obedecer a finalidade comunicada ao interessado antes de sua coleta;

d) princípio da publicidade: ao se admitir a máxima circulação das informações, deve-se, ao mesmo tempo, permitir os interessados exercitar um real poder de controle obre a exatidão dessas informações e sobre sua utilização;

e) princípio da segurança física e lógica da coletânea de dados: os dados pessoais devem ser protegidos contra riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado;

f) princípio da temporalidade: os dados fornecidos não podem ser conservados além do tempo necessário para consecução da finalidade especificada. Acrescenta-se ainda os princípios da relevância e da proporcionalidade, segundo os quais a coleta e dados pessoais deve ser mínima.

A indicação desses princípios baliza as práticas para coleta e tratamento de dados pessoais que, no território nacional, clama por uma proteção equitativa a de direito fundamental, uma vez que a atividade extrai elementos que pertencem ao conjunto de partes representado pela unidade do valor e integridade de uma pessoa (MORAES, 2003).

Sendo assim, imersos nessa nova era, a proteção aos dados pessoais só poderá ser fluída se houver confiança dos titulares perante as novas tecnologias da informação, fruto da globalização.

Portanto, o quadro jurídico resulta na observação do trato da legislação infraconstitucional vigente que tutela e diferencia dados pessoais de dados sensíveis, estabelecendo limites para o tratamento e respeitando, como fundamento, a privacidade do titular de dados.

1.2. Comparando dados pessoais com dados sensíveis e sua identificação prática na saúde

A proteção aos dados pessoais é parte integrante do quadro legislativo, e, consectário da cláusula geral de tutela da pessoa humana e do direito à privacidade, também é elemento essencial a democracia (MULHOLLAND, 2018).

Por outro lado, o exponencial de tecnologias cada vez mais avançadas, deu ordem na mesma relação ao aumento da capacidade de tratamento de dados pessoais das mais variadas tipologias, mediante o uso de algoritmos altamente sofisticados e a possibilidade de prever situações mediante o uso de técnicas de aprendizado por máquinas (do inglês, *Machine Learning*) (MULHOLLAND, 2018).

Assim, voltados à uma normatização adequada e preocupada com a imposição de limites ao tratamento de dados pessoais, é primordial conceituar dado e o que podem ser considerados dados pessoais.

O ponto de partida é a definição trazida por Castro (2005) que alude dado pessoal como: "*qualquer informação (numérica, alfabética, gráfica, fotográfica, acústica), independentemente do suporte (som e imagem), referente a uma pessoa identificada ou identificável*."

Dado pode ser caracterizado como uma unidade segmentada detentora de certo valor informacional, sendo que a classificação de um dado como pessoal indica características atribuídas a um indivíduo, as quais refletem fragmentos de sua própria identidade. A delimitação da classificação semântica de dados pessoais pode ser fundamental para legislações que pretendam regular a proteção de dados pessoais, posto que, a depender dessas marcações conceituais, pode se verificar uma maior ou menor amplitude do alcance da própria personalidade humana. Nesse sentido, as definições de dados pessoais podem ser consideradas expansionistas ou reducionistas (BIONI, 2016).

As definições reducionistas encerram um conceito restritivo, segundo as quais um dado é aquele capaz de identificar, de maneira individualizante, uma pessoa. Dessa forma, o dado pessoal refere-se de maneira única a uma pessoa específica (identificada), não restando dúvidas a respeito da relação entre o dado e o indivíduo ao qual se refere (BIONI, 2016). O Quadro 01 apresenta um exemplo de dados pessoais.

Quadro 01: Representação de Dados Pessoais

A) Nome	B) CPF	C) CEP	D) Idade	E) Profissão
1.Bianca Amorim	453.887- 43	80478-00	18	Estudante
2.Bianca Amorim	342.443.-11	04530-11	31	Jornalista
3.João Amorim	934.913 -32	64545-29	45	Médico

Fala-se, portanto, que o dado pessoal detecta uma pessoa dita "identificada" de maneira clara, por meio de identificadores numéricos únicos que, inequivocamente, invocam uma informação pessoal de um determinado indivíduo (BIONI, 2016).

No Quadro 01, a união de dados representa a evidente identificação de uma determinada pessoa. Entretanto, para o conceito do reducionismo, o mínimo de elementos já seria suficiente para identificar de maneira direta e exata quem se

pretende. Essa afirmação pode ser confirmada quando somadas as variáveis “nome” e “CEP”, das colunas “A” e “B”, respectivamente, de maneira a individualizar inequivocamente o sujeito. (BIONI, 2019).

Por outro lado, a acepção expansionista amplia o conceito de dado pessoal e para que um dado possa ser caracterizado como tal, não é imprescindível que sua capacidade de identificar um indivíduo seja plena e inequívoca (BIONI, 2019).

Utilizando ainda como base o Quadro 01, à título exemplificativo e para melhor compreensão, agora para indicar a ação expansionista, na hipótese de haver supressão da variável “CPF” restariam incertezas a respeito de qual dos indivíduos da coluna “Nome” exerce a profissão de “jornalista”, presente na coluna “Profissão”. Nessa definição, portanto, se verifica que a análise aos dados pessoais de cada unidade informacional é dada de maneira indireta, imprecisa, inexata e mediata para identificar uma pessoa identificável (BIONI, 2019).

A recente entrada em vigor da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709 de 2018), em setembro de 2020, reserva o primeiro inciso do art.5º para conceituar o que considera ser um dado pessoal: “informação relacionada a pessoa natural identificada ou identificável”.

Assim, como visto, o mecanismo de cruzamento de dois ou mais dados se aproxima da condição de reversão do anonimato do sujeito, podendo identifica-lo ou torna-lo identificável.

A saber da conceituação de dados pessoais percorrida até aqui, importante ressaltar outra hipótese de dado pessoal atribuída pela LGPD, qual seria de compreender o significado de “dados pessoais sensíveis”.

Na expressão da própria legislação, o dado pessoal sensível está conceituado no inciso segundo do art. 5º da LGPD que o classifica como um “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018).

Ainda, Bioni (2019) acrescenta que os dados pessoais sensíveis podem ser considerados aqueles relacionados à personalidade do indivíduo e suas escolhas pessoais, de modo que seu conteúdo pode oferecer uma especial vulnerabilidade: a discriminação

Essa visão é explorada ainda por Mulholland (2018, p. 176) ao defender que a definição de dado pessoal sensível não deve ser realizada meramente com a observação de sua natureza, mas também deve ser levado em consideração o potencial discriminatório que possuem as operações com este dado, diferentemente do que ocorre na utilização de dados pessoais não sensíveis em que, na maioria das vezes, não possui essa preocupação.

Nesse aspecto, o legislador preocupou-se em elencar no inciso II do art. 5º da Lei nº13.709 de 2018 – LGPD os dados que sugerem maior grau de discriminação social, especialmente pelo uso das tecnologias, os quais exprimem orientação sexual, religiosa, racial, estado de saúde ou filiação sindical (BRASIL, 2018).

Apesar da LGPD ter trazido um conceito aplicado de dados pessoais sensíveis, o seu tratamento jurídico já é conhecido na legislação brasileira desde a promulgação da Lei de Cadastro Positivo – Lei nº 12.414/11, no art. 3º, § 3º, II, a qual proíbe anotações em bancos de dados usados para análise de crédito com base em "informações sensíveis, assim consideradas aquelas pertinentes à origem social e ética, as saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas." (BRASIL, 2011). Significa, portanto, que para fins de análise de concessão de crédito, princípio da finalidade, estão vedadas inclusões nas bases de dados e quaisquer informações de natureza personalíssima que não se relacione à finalidade almejada com a análise de crédito, com o objetivo de evitar o tratamento discriminatório, a partir da aplicação do princípio da não discriminação (MULHOLLAND, 2018).

A importante ressalva feita por Bioni (2019, p. 84) é que, num primeiro momento, os dados pessoais coletados podem não parecer sensíveis, mas, em razão do contexto dado à sua coleta, podem permitir conduzir à outras informações de cunho discriminatório. Isso se deve, especialmente, quando se tem à disposição as TIC's e acessibilidade que permitem correlacionar uma série de dados suficientemente capazes de predizer comportamentos e acontecimentos.

Uma situação que exemplifica essa afirmação é a coleta de dados de geolocalização em dispositivos móveis de uma pessoa que está semanalmente em uma determinada igreja ou espaço de culto. Inicialmente, a funcionalidade seria apenas para rastreamento do aparelho e/ou dispositivo móvel, entretanto, considerando a forma como esses dados poderão ser utilizados, a vulnerabilidade

confere risco aos dados sensíveis, nesse caso sobre a convicção religiosa do indivíduo.

Pela expressão da LGPD, para que haja tratamento de dados pessoais sensíveis é necessário que o agente fundamente a necessidade, levando em consideração as hipóteses legais previstas no art.11º, seguido da observação da boa-fé e demais princípios elencados nos incisos do art. 6º (BRASIL, 2018).

No que se refere aos requisitos para tratamento de dados sensíveis, a LGPD traz as seguintes hipóteses[3]: a) consentimento do titular; b) obrigação legal, c) necessidade para formulação de políticas públicas, d) estudo por órgão de pesquisa, e) exercício regular de direito em processo, f) proteção da vida ou incolumidade física, g) tutela da saúde por profissionais de saúde, e g) garantia de prevenção a fraude e à segurança do titular (BRASIL, 2018).

---

[3] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
I - a portabilidade de dados quando solicitada pelo titular; ou
II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Particularmente, com relação ao consentimento, a LGPD define que ele deve ser livre, informado e com finalidade determinada (art.5º, inciso XIII) (BRASIL, 2018). O termo livre alude a um ato do titular independente de coação física, moral, mental ou artificio que o induza. O fato de ser informado exige que o titular seja comunicado acerca do uso e compartilhamento e seus dados de forma clara e de fácil entendimento. Já a finalidade, refere-se à necessidade de demonstração clara e específica sobre quais serão as utilidades do tratamento dos dados, sendo vedadas autorizações genéricas e utilizações incabíveis ao contexto (BIONI, 2015). Por outro lado, em diversos países da União Europeia tem sido preconizado, acessoriamente, o denominado consentimento ativo, que consiste na vedação da obtenção do consentimento de forma implícita por inércia do titular de dados em não se opor ao tratamento.

Os dados coletados por hospitais e clinicas de atendimento de saúde, em sua maioria, são dados pessoais sensíveis e o consentimento do paciente inclina-se à necessidade do atendimento e aos aspectos éticos que compreendem a atuação profissional médica na guarda e sigilo dessas informações.

Ocorre que, além desses dados explicitamente informados, o ramo de saúde também está subordinado ao cumprimento de demandas administrativas padrões que exigem o repasse de dados destes pacientes aos órgãos públicos e privados, quando necessário.

Por vezes, o consentimento do paciente e também titular de dado, não compreende essa extensa comunicação. De modo que, na hipótese de repasse de dados nessas condições, ainda que a título gerencial, a custódia dessa informação estaria sob responsabilidade de um administrador desautorizado pelo titular para operar, oferecendo a ele perigo.

Atualmente, no Brasil, cada serviço vinculado ao Sistema Único de Saúde (SUS) possui autonomia para desenvolver um modelo próprio de consentimento e assentimento informado para a realização de consultas, exames e procedimentos médicos. Em análise feita por Aragão e Schiocchet (2020) se confirma a inexistência de padronização ou exigência de requisitos mínimos para a coleta e tratamento de dados em si, tampouco para o armazenamento, seja ele físico ou digital.

Considerando a diversidade de procedimentos, cada instituição de saúde padroniza seus próprios procedimentos internamente e faz uso de terminologias específicas para se referir aos seus procedimentos práticos, por exemplo, a realização

de uma intervenção cirúrgica, anestesias, parto e intervenções obstétricas, amputações, exames videolaparoscópicos, recusa de tratamento medicamentoso e/ou invasivo, abandono de tratamento, alta médica, dentro outros, o que demanda uma dificuldade na padronização, devendo, cada instituição, analisar suas necessidades.

Outro elemento essencial para o tratamento de dados sensíveis é, sem dúvida, a confidencialidade, que corrobora com os princípios éticos basilares para o exercício da atividade profissional na área. Essa questão esbarra em uma outra preocupação bastante latente dentro do aspecto de saúde: o livre compartilhamento e dados e informações entre instituições componentes ou correlatas. Esse ponto crítico vai ao encontro da implementação da Lei Geral de Proteção de Dados Pessoais visto que, em diversas situações, seja no âmbito público ou privado, os sistemas operam de maneira setorizada, disponibilizando, assim, informações sobre o paciente para outros setores.

Ainda, a respeito do intercâmbio de dados, no próprio Poder Judiciário surge exigências de prestar informações e esclarecimentos de dados sensíveis, seja por meio do Ministério Público ou das Defensorias Públicas, de modo que a exposição desses dados em repartições diversas e desconhecidas fogem do controle e consentimento do titular.

Por vezes, esse fluxo é obstado por gestores ou profissionais que se veem inseguros diante de vazios regulamentares, da omissão legal e da ausência de normatização e padronização dessa sistemática, uma vez que o conteúdo é estritamente particular e circula em sistemas com diversidade de acesso.

Mesmo que a LGPD tenha trazido uma inovação com a tipologia do “dado anonimizado”, art. 5º, inciso III (BRASIL, 2018), na tentativa de sugerir maior segurança diante da impossibilidade de revelar a identidade de seu titular, no entanto, a norma esclarece que os dados anonimizados não serão considerados pessoais, salvo se o processo de anonimização for revertido (art. 12, LGPD) (BRASIL, 2018).

Em evidência, a anonimização do dado é resultado da descaracterização individual ocasionada pela quebra do vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), se comportando em antítese ao conceito de dado pessoal já apresentada (BIONI, 2019).

Para a adoção de medidas de saúde pelo ente público ou privado, raramente é aplicável a anonimização de dados, uma vez que o tráfego de dados e informações

pelo meio digital ou físico favorece o alcance de profissionais capacitados para conduzir o paciente ao melhor procedimento e tratamento médico. Unir os fatores de sigilo e confidencialidade diante de situações de extrema necessidade de saúde, nem sempre é tarefa fácil.

A cartilha do Conselho Federal de Medicina (CFM), em parceria com a Sociedade Brasileira e Informática em Saúde (SBIS), lançada em 2012, orienta os profissionais acerca da necessidade de certificação dos sistemas de registro eletrônico de saúde, como forma de garantir a segurança e a confidencialidade das informações do paciente (CFM, 2012). Além do mais, orienta ao uso de mecanismos correlacionados à segurança de rede, criptografia de dados, monitoramento de acesso e assinaturas digitais, simultaneamente às certificações de segurança, como forma de tornar mais concreta a privacidade de dados pessoais dos usuários.

Complementar à cartilha, a Resolução nº 1821/2007, importante marco regulatório para a categoria, também apontava o Conselho Federal de Medicina como Autoridade Certificadora (AC) dos médicos brasileiros, instituía o Prontuário Eletrônico do Paciente (PEP) e Registro Eletrônico de Saúde (RES), além de garantir que os interessados receberiam a identificação profissional (CRM-Digital) com um certificado padrão ICP-Brasil (CFM, 2007).

Recentemente, iniciada a transmissão local do novo coronavírus no Brasil, o Ministério da Saúde, por intermédio da Portaria nº 188/2020 declarou “emergência na saúde pública de importância nacional” (BRASIL, 2020). Com a imposição do distanciamento social como medida de contenção à proliferação do vírus (OMS, 2020) o presidente da República sancionou a Lei nº 13.989/20, em caráter emergencial e de vigência temporária, conferindo ao exercício da medicina o uso de tecnologias “para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção da saúde” (BRASIL, 2020). Nesse período, a Resolução do CFM nº 2.227 de 6 de fevereiro de 2018 permaneceu em vigor até 26 de fevereiro de 2019, quando foi revogada por força da Resolução 2.228.

A primeira dispunha sobre as práticas de atendimento aos pacientes mediante o uso de novas tecnologias por meio da plataforma e-Saúde respeitando a privacidade e as informações cedidas. Ademais, dentre as diversas práticas, o e-Saúde engloba igualmente o teleatendimento, as teleconsultas e videoconferências, as telecirurgias, a tele-educação, bibliotecas virtuais e imagens, o desempenho de segundas opiniões

formativas, dentre outras atividades que reforçam a qualidade do atendimento médico (REZENDE, 2010).

Sendo assim, no aspecto geral da regulamentação da proteção aos dados, sejam eles dados pessoais, dados pessoais sensíveis ou anônimizados, a aplicação da norma segue associada às premissas do direito constitucional à privacidade e igualdade e, em especial o dado sensível, ao rigoroso princípio da não discriminação (RODOTÁ, 2008).

Ainda, complementar aos princípios, a autodeterminação informativa segue como elemento acessório à condição de equilíbrio para a efetivação da igualdade e liberdade dos indivíduos e titulares de dados perante à sociedade, de modo que, na hipótese de assimetria desses elementos certamente se evidencia prejuízos à coletividade.

Portanto, resta saber como esses dados pessoais sensíveis alimentam os sistemas computacionais dos padrões utilizados para o suporte à saúde, e como esses dados deverão estar articulados com as medidas de segurança dos sistemas, a fim de evitar vulnerabilidades e riscos aos seus titulares.

1.3. Os sistemas computacionais padrões utilizados para a troca de dados em saúde

O conglomerado de dados e informações capturadas por instrumentos provenientes de tecnologias digitais da informação e comunicação (TDIC), tem provocado uma série de mudanças em todas as esferas da sociedade. A utilização de processos padronizados se faz presente nos mais variados segmentos do mundo organizacional, sendo considerada ferramenta fundamental no gerenciamento de tarefas (CAMPOS, 1992) de alta e baixa complexidade, possibilitando a manutenção da qualidade, redução de custos, e, aparentando maior grau de confiabilidade (FALCONI, 1992).

Na esfera da saúde, diversas vantagens e desvantagens derivam do processo de unificação de dados a partir da implementação do Registro Eletrônico em Saúde (RES) (BRASIL, 2017), que será melhor desenvolvido na sequência.

Frente ao considerável alcance da Internet e de melhores condições de acesso aos prontuários eletrônicos, o Ministério da Saúde por meio da Portaria nº 2.073 de 2011 autorizou e regulamentou o uso de sistemas padrões e interoperáveis

para o tráfego de informações de saúde tanto em âmbito público como privado (BRASIL, 2011).

Na disposição do art. 4º dessa mesma Portaria (BRASIL, 2011), foi instituído uma listagem de padrões, denominada de “Catálogo de Padrões de Interoperabilidade de Informações e Sistemas de Saúde (CPIISS)” a serem utilizados como parâmetro de comunicação em vocabulário, imagens, conteúdo e estrutura, representação de dados clínicos, segurança, autenticidade e qualidade. Dentre os padrões indicados no catálogo, pode-se citar como exemplos: OpenEHR[4], HL7[5], SNOMED-CT[6], TISS[7], HL7CDA[8], DICON[9], LOINC[10], ISBT 128[11], ISO 136062[12], IHE-PIX[13]; CID[14], CIAP-2[15], TUSS[16] e CBHPM[17] (BRASIL, 2011).

---

[4] OpenEHR: trata-se de um repositório digital de informações sobre a saúde das pessoas, possibilitando uma leitura, pelos profissionais de saúde, mais eficiente dos históricos clínicos. http:// www. openehr. org / home. html

[5] HL7: trata-se uma Organização Desenvolvedora de Padrões (SDOs) internacional, que opera na área de Sistemas de Informação em saúde, tanto para a área clínica, como administrativa. https://hl7.org.br/

[6] SNOMED-CT: trata-se de sistema para codificação de termos clínicos e mapeamento das terminologias nacionais e internacionais em uso no país, visando suportar a interoperabilidade semântica entre os sistemas. https://www.snomed.org/snomed-ct/why-snomed-ct

[7] TISS: trata-se de Troca de Informações em Saúde Suplementar (TISS) utilizado em sistemas interoperáveis. https://www.gov.br/ans/pt-br/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-2013-tiss/padrao-tiss-2013-agosto-2021

[8] HL7CDA: trata-se de sistema para definição da arquitetura do documento clínico padrão. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7

[9] DICOM: trata-se de sistema utilizado para a padronização de representação da informação relativa a exames de imagem. https://www.dicomstandard.org/

[10] LOINC: trata-se de padrão para a codificação de exames laboratoriais. https://loinc.org/

[11] ISBT 128: trata-se de sistema para a codificação de dados de identificação das etiquetas de produtos relativos ao sangue humano, de células, tecidos e produtos de órgãos. https://bvsms.saude.gov.br/bvs/publicacoes/plano_implantacao_padrao_ISBT128.pdf

[12] ISO 136062:2019 : trata-se de padrão de interoperabilidade de modelos de conhecimento, incluindo arquétipos, templates e metodologia de gestão. https://www.abntcatalogo.com.br/norma.aspx?ID=418193

[13] IHE-PIX: trata-se de sistema para cruzamento de identificadores de pacientes de diferentes sistemas de informação. http://openpixpdq.sourceforge.net/

[14] CID: trata-se da *International Classification of Diseases* (ICD), traduzida para Classificação Internacional de Doenças (CID) em que se objetiva a padronização e criação de códigos para indicar doenças, sintomas, denúncias, circunstâncias socias e causas externas de dados/doenças.

[15] CIAP-2: trata-se de um sistema de Classificação Internacional de Atenção Primária – Segunda Edição (CIAP2) utilizado como ferramenta para atendimentos relacionados às pessoas, e não a doenças, na saúde primária. https://www.sbmfc.org.br/ciap-2/

[16] TUSS: trata-se de Terminologia Unificada em Saúde Suplementar (TUSS) com o objetivo de padronizar todas as nomenclaturas e códigos ligados à procedimentos médicos. http://www.ans.gov.br/images/stories/Legislacao/in/anexo_in34_dides.pdf

[17] CBHPM: trata-se da Classificação Brasileira Hierarquizada de Procedimentos Médicos (CBHPM) utilizado como parâmetro para cálculo de consultas e procedimentos médicos. https://amb.org.br/cbhpm/

Entre todos esses padrões a pesquisa se concentrou nos padrões TISS e TUSS, visto que são utilizados para o gerenciamento de planos de saúde suplementar, e os dados pessoais que os alimentam podem vir a identificar o paciente e o procedimento realizado, tornando-o um dado pessoal sensível sob a exigência de critérios legais. . Para melhor explorar a definição de cada padrão existente, é essencialmente necessário iniciar pela definição de interoperabilidade.

A conceituação mais referenciada sobre interoperabilidade tem origem no Departamento de Defesa dos EUA (DoD), publicada em 1977, que define a interoperabilidade como "*the condition achieved among communications-eletronics systems or items of communications-eletronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their uses*"[18] (DoD JP1-02,2010).

Nesse sentido, Marcondes e Sayão (2008, p. 136) refletem que a interoperabilidade é a possibilidade de o usuário buscar por recursos informacionais heterogêneos, armazenados em diferentes locais de uma rede, utilizando-se de uma interface única e sem necessidade de conhecimento sobre como os recursos estarão armazenados. Complementando, Arms (2002) explica que a interoperabilidade tem o objetivo de desenvolver serviços e soluções úteis para os usuários, a partir de recursos informacionais que são tecnicamente diversos, e muitas vezes gerenciados por instituições diferentes.

Na perspectiva de Uklon (2005) e Miller (2000) a interoperabilidade é entendida como um processo contínuo focado em garantir que os sistemas, procedimentos e a cultura de uma organização sejam conduzidos com o fim de maximizar oportunidades de intercâmbio e reutilização da informação, seja de maneira interna ou externamente.

A interoperabilidade aplicável aos sistemas de saúde configura ampla capacidade dos gerenciadores de informação para trabalhar em conjunto nas ações de coleta, processamento, registro e busca de dados e informações interligando espaços físicos e superando fronteiras organizacionais.

---

[18] Tradução livre para: "a capacidade de sistemas, unidades, ou forças de disponibilizarem serviços para, e aceitarem serviços de outros sistemas, unidades ou forças e de utilizarem estes serviços no sentido de operarem eficazmente em conjunto"

O ato de padronizar sistemas, para Sales e Pinto (2019) está diretamente atrelado à capacidade de torná-lo interoperável, autorizando assim a troca de informações essenciais, como ocorre no setor saúde.

Portanto, quando há a compreensão de que o intercâmbio de dados e informações de conteúdo médico e operacional podem ser capazes de promover a eficácia na prestação de serviços individuais, voltados para cada paciente, e também aos serviços coletivos, direcionado ao bem estar social, o padrão é adotado pelas organizações (SALES; PINTO, 2019).

Importante ressaltar que a interoperabilidade opera na coexistência de sistemas, por vezes, heterogêneos, ou seja, que se apresentam em descontinuidade entre si. Nessa hipótese, os modelos de dados, a linguagem, imagem, representações e plataformas são diferentes, no entanto, necessitam comunicar-se. Como solução, Pasqual e Sunye (2003) apontaram a utilização da linguagem XML (do inglês, *eXtensible Markup Language*) com capacidade prática em descrever o dado de maneira versátil e com entendimento universal em DTD (*Document Type Definition*), que será aprofundado no Capítulo seguinte.

Com a autorização da Lei nº 13.787 de 2018, a disponibilização do Prontuário Eletrônico do Paciente (PEP) passou a ser considerada legal, levando em consideração a possibilidade de resguardar os dados e as informações de saúde do paciente, incorporando ao Registro Eletrônico de Saúde (RES) (BRASIL, 2018).

Para suprir essa necessidade do compartilhamento e disponibilidade de dados de saúde de pacientes, além dos padrões autorizados pelo Ministério da Saúde, também são destaque alguns padrões internacionais, a exemplo do: HL7 e OpenEHR.

Considerando o entendimento sobre a interoperabilidade, passa-se a explicar os padrões internacionais e nacionais voltados ao intercâmbio de dados de saúde de pacientes entre sistemas, considerando também o Registro Eletrônico de Saúde (RES).

Como padrão internacional, explica-se primeiramente o *Health Level Seven* (HL7) o qual advém de uma organização voluntária, sem fins lucrativos, fundada em 1987, sendo que em 1994 foi reconhecida internacionalmente pelo ANSI-SDO (*American National Satandards Institute – Standards Developing Organizations*). Seu objetivo é promover normas para a interoperabilidade de sistemas de saúde para aperfeiçoar o atendimento clínico, otimizar o fluxo de trabalho, reduzir ambiguidade e

permitir a transferência de conhecimento entre profissionais de saúde, agências governamentais, indústria e pacientes (HL7, 2009).

Inicialmente, a utilização do padrão HL7 foi subdivida em duas categorias: versão 2 (V2) e versão 3 (V3). O padrão HL7 V2 foi criado principalmente por especialistas em interfaces clínicas e projetado para fornecer uma estrutura na qual os dados podem ser trocados entre diferentes sistemas clínicos. Já o padrão HL7 V3 teve sua criação influenciada pelo governo e usuários de informações médicas. Inicialmente considerou-se uma adesão mundial desse padrão, entretanto, até o momento, o V3 permanece incompatível ao V2, o que indica que ele não foi amplamente adotado.

Decorrente do HL7 foi criado o *Clinical Document Architecture* (CDA), padrão de marcação responsável pela troca, gerenciamento e integração entre sistemas de informação de saúde, utilizado tanto para agregar informações clínicas como administrativas.

Recentemente, a organização sugeriu a inserção de um novo padrão no mercado: o HL7 *Fast Health Interoperable Resources* (FHIR) que combina os melhores recursos do HL7 V2, HL7 V3 e HL7 *Clinical Document Architecture* (CDA) atrelado as inovadoras tecnologias de serviços web.

Outro modelo internacional utilizado para padronizações em sistemas de saúde é o OpenEHR. Esse abrangente modelo consiste em um conjunto de especificações e ferramentas livres para registros clínicos que podem ser aderidos em módulos, de acordo com a necessidade e, ainda, permite que as operações modulares conversem através do sistema interoperável (OPENEHR, 2021). Esse modelo também está em conformidade às normas ISO/IEC nº 13606-2 (ISO/IEC,2019), que especifica a arquitetura de informações necessárias para comunicações interoperáveis entre sistemas e serviços de que necessitam para o preenchimento do *Eletronic Health Record* (EHR) ou Prontuário Eletrônico do Paciente (PEP).

Vale ressaltar que as normas ISO são consideradas balizadoras no desenvolvimento de sistemas, visto que consistem em admitir uma padronização conceitual e sistemática de reconhecimento internacional aos diversos setores de atuação, conferindo maior credibilidade aos padrões propostos.

Em específico aos padrões de saúde, o ISO/IEC nº 13606-1 (ISO/IEC, 2008) possui como foco primário na comunicação entre diferentes Registros Eletrônicos de Saúde (RES) e, além disso, serve ainda de base para a implementação de outros

padrões. Inclusive, a ISO/TR nº 20514 (ISO/TR, 2015) está voltada às aplicações de informática na saúde e define, em específico, a respeito dos Registros Eletrônicos em Saúde (RES), além de fornecer descrições de apoio voltadas reforçar as características padrões dos sistemas de registro.

Os padrões desenvolvidos na saúde, sejam eles organizados por grupos e/ou organizações especializadas, ou também aqueles criados por interesse da própria entidade governamental, podem funcionar de maneira isolada. Entretanto com a vasta ampliação de produtos no mercado, torna-se imprescindível que os padrões atuem em conjunto, de maneira interoperável.

A criação de padrões enfrenta diversas fases, a exemplo de: necessidade, conceituação, discussão, processo aberto, implementação, manutenção, disseminação, teste de conformidade, entre outras; o que os torna, em geral, um processo oneroso e com adversidades. No Brasil e Estados Unidos da América o trabalho desenvolvido é voluntário, com significativa redução dos custos de produção, o que contribui para que o resultado atenda às necessidades e interesses do grupo pesquisador. Em outros locais, a exemplo da Europa, o desenvolvimento desses sistemas é de interesse do próprio Estado que fomenta, incentiva e, consequentemente, prioriza seus interesses.

Nacionalmente, os padrões que se voltam a atender as necessidades da saúde interagem na utilização pela saúde pública e saúde privada. Os mais explorados e utilizados pelo senso comum, são: Troca de Informações em Saúde Suplementar (TISS) e a Terminologia Unificada da Saúde Suplementar (TUSS).

Em 2007, a Agência Nacional de Saúde lançou a Resolução Normativa nº 153, a qual estabelecia a troca de informações na Saúde Suplementar (TISS), como um padrão obrigatório para as trocas eletrônicas de dados de atenção à saúde dos beneficiários de planos entre os agentes da saúde suplementar. O desenvolvimento desse padrão iniciou-se em maio de 2003, a partir de um trabalho de pesquisa elaborado em convênio com o Banco Interamericano de Desenvolvimento (ANS, 2007).

Para melhor desenvolvimento do trabalho de pesquisa, a Agência Nacional de Saúde Suplementar (ANS) criou um grupo de trabalho para analisar os padrões e informações já existentes no mercado, visando assim propor um modelo único de troca de informações em saúde suplementar. Durante o período de realização das pesquisas, foram trocadas e analisadas diversas guias em papel dentro dos diversos

atores de mercado, além de um longo processo de visitas presenciais aos prestadores e operadores de planos de saúde com o intuito de identificar as dificuldades enfrentadas no processo de troca de informações (ANS, 2007).

Após cinco anos, a Resolução Normativa nº 153 de 2007 foi revogada, dando espaço para a Resolução Normativa nº305, de 9 de outubro de 2012, em vigor e que dispõe sobre a implementação de padrão para enquadramento de dados de atenção à saúde dos beneficiários de plano privado (ANS, 2012).

Segundo a ANS (2012) o padrão TISS se resume na interoperabilidade entre sistemas de informação em saúde recomendado pela ANS e o Ministério da Saúde e, ainda, proporciona a redução da assimetria de informações entre os atores da saúde suplementar. O padrão TISS se refere, especificamente, às trocas de dados decorrentes de ações de atenção à saúde prestada ao beneficiário de plano privado de assistência à saúde.

A troca de dados da saúde do beneficiário perante a rede de prestadores de serviços em saúde, tem as finalidades de: a) padronizar as informações administrativas de verificação, solicitação, autorização, cobrança, demonstrativos de pagamento e recursos de glosas; b) subsidiar à ANS em ações de avaliação e acompanhamento econômico, financeiro e assistencial das operadoras de planos privados de assistência a saúde; e, c) compor o registro eletrônico dos dados de atenção à saúde dos beneficiários de planos privados de assistência à saúde (ANS, 2012).

Entende-se como rede de prestadores de serviços de saúde da operadora de planos privados: a) a rede de serviços da contratada, referenciada ou credenciada, de forma direta ou indireta; e, b) a rede própria da operadora, de entidade ou empresa controlada pela operadora, de entidade ou empresa controladora da operadora e profissional assalariado ou cooperado da operadora (ANS, 2012).

Composto por cinco componentes indicados e representados no Quadro 02, o Padrão TISS, é organizado por um conjunto de regra operacionais. Tamanha sua importância com relação a proposta desta pesquisa, cada componente será cuidadosamente detalhado no Capítulo 2, item 2.3, estabelecendo uma relação com a proteção de dados e a segurança da informação.

Quadro 02: Componentes Operacionais do Padrão TISS

Componente	Descrição
Organizacional	Responsável por estabelecer o conjunto de regras operacionais.
Conteúdo e estrutura	Responsável por estabelecer a arquitetura dos dados utilizados nas mensagens eletrônicas e no plano de contingência, para coleta e disponibilidade dos dados de atenção à saúde.
Representação de Conceitos em Saúde	Responsável por estabelecer o conjunto de termos para identificar os eventos e itens assistenciais na saúde suplementar, consolidados na Terminologia Unificada da Saúde Suplementar – TUSS
Segurança e Privacidade	Responsável por estabelecer os requisitos de proteção para assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde. Tem como base o sigilo profissional e segue a legislação.
Comunicação	Responsável por estabelecer os meios e os métodos de comunicação das mensagens eletrônicas definidas no componente de conteúdo e estrutura. Adota a linguagem de marcação de dados XML.

Fonte: ANS, 2012

Com características gerenciais de dados, o TISS padroniza procedimentos, sejam eles: a verificação de elegibilidade; autorização de procedimentos; comunicação de internação; alta do beneficiário; cobrança de serviços de saúde; demonstrativo de retorno; recurso de glosa e comprovante presencial. Para garantir a confiabilidade, todos os procedimentos exigem uma mensagem de envio e outra de retorno, dessa forma é possível auferir que o conteúdo foi entregue com autenticidade (ANS, 2012).

Por sua vez, o padrão TUSS estabelece um formato para a utilização de nomenclaturas e, por isso, é considerado como continuação da funcionalidade do padrão TISS (ANS,2009). Isso porque, para que procedimento seja lido e concluído sem ruídos e assimetrias informacionais é necessário a padronização de nomenclaturas e códigos de procedimentos médicos feita com base na Classificação Brasileira Hierarquizada de Procedimentos Médicos (CBHPM). Durante muitos anos cada operadora de plano de saúde criava sua própria tabela baseado em interesses próprios. Após diversos prejuízos relacionados aos atendimentos prestados, surgiu a necessidade de criar a CBHPM para regulamentar e uniformizar a cobrança de determinados procedimentos médicos. Para tanto, mesmo que as terminologias e códigos-fonte utilizados no padrão TUSS sejam elaborados e atualizados pela ANS, é autorizado por lei que a operadora do plano de saúde suplemente essas informações, caso identifique a ausência (BRASIL, 2012).

Não há dúvidas de que a padronização de nomenclaturas e procedimentos gerenciais, a exemplo do Prontuário Eletrônico do Paciente (PEP) colaboram para a condução de procedimentos que envolvam a tríade entre o ambiente hospitalar ou clínico, o sistema eletrônico de armazenamento e, por fim, o paciente.

Mesmo com o avanço tecnológico, não é possível garantir que as modificações dos sistemas interoperáveis tenham sido corretamente atualizadas, podendo, como consequência, gerar incertezas quanto à segurança, celeridade e confiabilidade dos procedimentos.

Por essa razão, faz-se necessário a adesão de ferramentas adequadas de controle de acesso e de integridade da mensagem trocada a fim de preservar a segurança do titular de dados e do sistema computacional.

1.4. As ferramentas de boas práticas de segurança da informação utilizadas para a contenção de ameaças

Quando o tema são os sistemas computacionais e o compartilhamento de dados entre sistemas, em especial dados pessoais, é essencial adentrar ao entendimento dos protocolos de segurança dos quais esses sistemas deverão submeter-se para garantir ao titular a privacidade e integridade na guarda, armazenamento e compartilhamento desses dados e informações.

Algumas técnicas baseadas em tecnologia e engenharia social podem ampliar o arquétipo de Segurança da Informação de uma organização, seja mediante a implementação de uma política de segurança adequada, utilização de *firewall*, incentivo ao uso de sistemas de detecção de intrusão, criptografia, segurança física, dentre outros mecanismos.

Devido ao intenso avanço tecnológico confirmado por Peck (2021), o número de incidentes vem crescendo vertiginosamente, ressaltando, mais uma vez, a importância de incorporar medidas de Segurança da Informação física e operacional em organizações públicas e privadas.

A Segurança da Informação, conforme Beal (2005) é o processo de proteção da informação contra ameaças à sua integridade, disponibilidade e confidencialidade. Para garantir adequada proteção aos seus ativos de informação, é necessário que a organização empresarial e seus principais gestores levantem e selecionem soluções específicas adequadas ao modelo de negócio específico.

Grande parte dos dados que compreendem a estrutura informacional de uma organização, pública ou privada, são armazenados em computadores, o que evidencia a preocupação na confiabilidade de sistemas baseados em TI (Tecnologia da Informação). Da Silva Netto e Silveira (2007, p.377) afirmam que na medida em que essa a confiança no armazenamento de dados for destruída, o impacto pode ser comparável a destruição do próprio sistema. Pela capacidade que os dados, informação e conhecimento tendem a adicionar valor aos processos, produtos e serviços, estes também constituem recursos cada vez mais críticos para o alcance da missão e do objetivo organizacional (CARUSO; STEFFEN, 1999).

Assim, para o melhor enfrentamento de vulnerabilidades, redução de ameaças, riscos e exposições, é necessário construir um conjunto adequado de controles, orientado por políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware capazes de agir como medidas agregadas à cibersegurança (HINTZBERGEN, et.al, 2018).

A cibersegurança, em sentido estrito, é definida como conjunto de atividades que se destinam a proteger sistemas informáticos (tal como definido no art. 2º da Lei nº12.737/2012 (BRASIL, 2012) e os dados informáticos neles contidos, mantendo-se à salvo da ocorrência de dano intencional ou do uso negligente (BRAVO, 2021).

Para formar o entendimento de processos para a Gestão de Segurança da Informação, as normas ISO (Organização Internacional de Padronização) e IEC (Comissão Eletrotécnica Internacional) formam o sistema especializado para padronização mundial e, em mútuo interesse, estabelecem campos específicos de atividade técnica (DISTERER,2013).

Dessa forma, o ISO/IEC 27001 integra a família de normas ISO/IEC 27.000, como demonstrado nas especificações do Quadro 03.

Quadro 03: Normas ISO/IEC da família 27000.

Norma ISO	Conteúdo
ISO 27000	Generalidades, definições e diretrizes
ISO 27001	Técnicas de segurança para Sistemas de Gestão da Segurança da Informação (SGSI)
ISO 27002	Boas práticas para SGSI
ISO 27003	Diretrizes para implantação de um SGSI
ISO 27004	Indicadores de desempenho do SGSI
ISO 27005	Gestão de riscos de segurança da informação
ISO 27006	Requisitos e normas para organizações de auditoria e certificação pela ISO 27001/2
ISO 27007	Diretrizes para auditoria ISO 27001/2
ISO 27008	Diretrizes para auditoria de controles de SGSI
ISO 27010	Guia para a comunicação em gestão da segurança da informação
ISO 27014	Técnicas para governança da segurança da informação
ISO 27017	Controles específicos para computação em nuvem
ISO 27701 (antiga 27552)	Requisitos e exigências para estabelecer um Sistema de Gerencia-mento de Informações de Privacidade

Fonte: Adaptado de https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html

A norma internacional ISO/IEC 27001 considera a Gestão de Segurança da Informação (SGSI) um processo estruturado que permite garantir os principais requisitos de segurança para o fluxo da informação, fornecendo um modelo para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) (ISO/IEC 27001, 2005).

Ao mesmo tempo, a ISO/IEC 27001 fomenta a adoção de uma abordagem por processos, que tem por orientação a utilização de um modelo que permite planejar, executar, verificar e atuar sobre todos os processos do SGSI, conhecido como modelo PDCA (*Plan – Do – Check – Act*) (ISO/IEC 27001,2005), conforme mostrado na Figura 01.

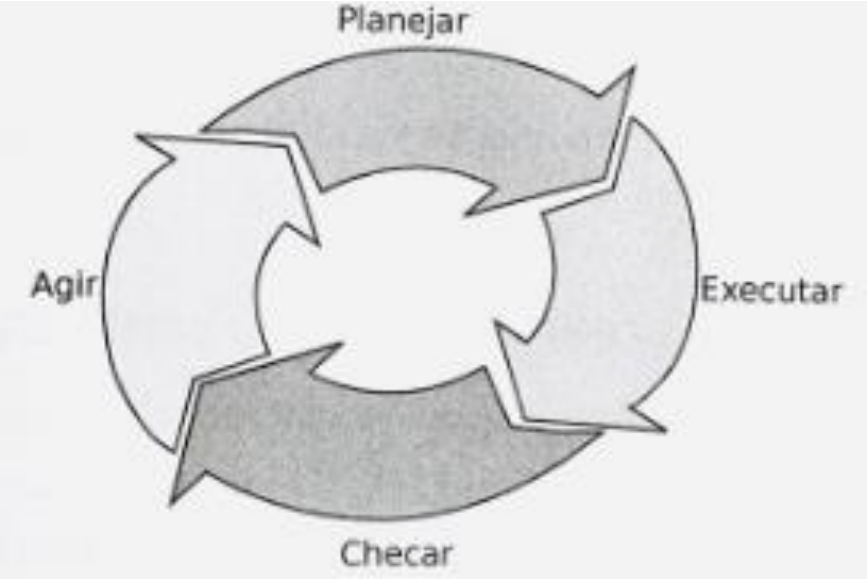

Figura 01: Ciclo PDCA (HINTZBERGEN et.al., 2018)

O modelo PDCA, também chamado de Ciclo de Qualidade de Deming, forma a base para implementar o sistema de gerenciamento de segurança da informação (HINTZBERGEN et.al., 2018). As etapas do ciclo de gerenciamento PDCA consistem em:

1) Planejar (*plan*): após uma breve identificação do problema-oportunidade, é realizado um consistente levantamento de dados e informações, para que, assim, o escopo deste projeto de correção, prevenção ou de melhoria possa se tornar o mais completo possível. Através das informações contidas no escopo, o problema será analisado (a partir do uso de ferramentas de qualidade, como o fluxograma, histograma, diagramas, etc.) e as soluções para resolvê-lo serão conhecidas e inseridas em um plano de ação;

2) Executar (*do*): municiado com o plano de ação para a solução do problema, a tarefa seguinte é colocar, de fato, as estratégias em funcionamento. É nessa fase que os resultados são gerados, e estes dependem da qualidade das ações e do nível de execução do plano de ação.

3) Avaliar (*check*): nessa etapa faz-se uma reflexão sobre os resultados colhidos até o momento e sobre o comprometimento dos responsáveis com a implementação das ações definidas.

4) Agir (*act*): após a execução, nesta etapa são aplicadas as ações para corrigir aquilo que foi identificado como errado na etapa anterior e, continuamente, aperfeiçoar o processo. Para que os problemas evidenciados não retornem

futuramente, pode ser implementado sistemas padrões, controles de processos estáticos e diversas outras ferramentas para a manutenção de melhoria e mitigação de vulnerabilidades não conhecidas.

O que era exigido pela norma ISO/IEC de 2005, facultou a utilização do PDCA, uma vez que cada empresa, na medida de suas características próprias, possui seu próprio ciclo de gestão de negócios, não estando obrigatoriamente baseado no PDCA (HINTZBERGEN, et.al, 2018).

Cabe destacar especialmente ligada à temática dessa pesquisa a ISO/IEC 27002:2013, pertencente à família ISO/IEC 27.000 que dispõe sobre o “código de prática para a segurança da informação”, incluindo alguns aspectos importantes da implementação gerencial: a) a compreensão de requisitos de segurança da organização; b) necessidade de estabelecer políticas e objetivos para a segurança da informação; c) implementação e operação de controles para gerenciar os riscos de segurança da informação da organização; d) monitoramento e revisão do desempenho e eficácia do Sistema de Gerenciamento de Segurança da Informação (SGSI); e) manutenção para melhoria contínua com base em medições objetivas (HINTZBERGEN, et.al, 2018).

Considerando o contexto de compartilhamento de informações de saúde entre sistemas interoperáveis de organizações médicas e hospitalares, há a preocupação para a garantia do bom funcionamento dessa operação específica de tratamento de dados.

Embora no âmbito nacional não existam legislações e regulamentos aplicáveis a todos os tipos de organizações, Peck (2021, p. 44) afirma que em determinados setores e tipos de serviços, há obrigações específicas no tocante a Segurança da Informação e à segurança cibernética. Contudo, além da implementação de normas técnicas nesse sentido, em especial para a padronização e organização de setores com reconhecimento internacional, outra prática possível às empresas é a implementação do Sistema de Gestão da Segurança da Informação (SGSI) para introduzir controles (PECK, 2021).

Para Edison Fontes (2012), o SGSI pode abranger o todo ou parte do processo organizacional, com a finalidade expressivamente voltada a proteção das informações da empresa obedecendo às propriedades: confidencialidade, integridade e disponibilidade (CID).

Assim, para o armazenamento ou manipulação de dados e informações, sejam elas públicas, internas ou confidenciais, os princípios CID devem ser observados para a mitigação de riscos eminentes (PECK, 2021).

As normas ISO/IEC 13335-1[19], define a: 1) confidencialidade: como propriedade de que a informação não esteja disponível ou que seja revelada a indivíduos, entidades ou processos não autorizados[20]; 2) integridade: como propriedade de salvaguarda da veracidade ou originalidade de ativos[21]; 3) disponibilidade: como propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada[22].

Todas as medidas de implementação, monitoramento, análise, manutenção e melhoramento da Segurança da Informação dentro de uma organização incorporam-se na redução do risco ou ao seu gerenciamento. (HOEPERS, 2011). Entretanto, de acordo com Varian (2004), muitos problemas de segurança da informação estão ligados à incentivos econômicos.

Na vigente Lei Geral de Proteção de Dados Pessoais se reforça a tutela aos direitos dos titulares de dados pessoais e são apontadas regras claras de boas práticas e governança (art. 50, §1º) para que todas as entidades públicas e privadas atendem e efetivem a proteção aos dados pessoais (BRASIL, 2018).

Nas condutas adotadas por uma empresa, organização ou corporação englobam diversas ações de “boas práticas” essenciais para reforçar as barreiras de segurança, porém, como ficou provado nos países da União Europeia que consolidaram o Regulamento Geral de Proteção de Dados Pessoais (UNIÃO EUROPEIA, 2016), o processo deve ser implementado gradualmente pois demanda tempo e investimento (CORTEZ; KUBOTA, 2013).

Dos elementos que se apresentam como mitigadores de ricos ou solucionadores das inquietações sobre segurança de sistemas e proteção à informação, encontra-se a: criptografia. Considerada a mantenedora da confidencialidade da informação, o termo criptografia é de origem grega e consiste da

---

[19] ISO/IEC 1333-1. Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management. 2004. p. 03. Disponível em: https://www.iso.org/standard/39066.html. Acesso em 24 de set 2021

[20] Texto original: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[21] Texto original: the property of safeguarding the accuracy and completeness of assets.

[22] Texto original: the property of being accessible and usable upon demand by an authorized entity

combinação das palavras “*kryptós*”, que significa “escondido”, e “*gráphein*”, que significa “escrita”. (HINTZBERGEN, et.al, 2018).

A principal razão para escolher a criptografia é a de manter a informação confidencial e os dados íntegros, além de garantir a garantia a autenticidade da mensagem. (HINTZBERGEN, et.al, 2018).

A criptografia também age no controle de acesso de usuários mediante a utilização de senhas, possibilitando a setorização para atender o princípio do menor privilégio. Nesta ação, todos os pedidos de acesso são documentados, com a finalidade de conferir a confiabilidade do contratante, (MARTINS; SANTOS, 2005).

Existem diversos sistemas criptográficos que podem ser utilizados para atender diferentes propósitos dentro da uma instituição, no entanto, é essencial que tal sistema esteja vinculado a um documento de políticas de boas práticas institucionais. A partir disso, é possível racionalizar como a criptografia será determinada dentro dos sistemas de informação da organização (DA SILVA NETTO; SILVEIRA, 2007).

O controle de acesso é institucionalizado pela chamada “chave criptográfica” Por meio de algoritmos, é possível converter um texto original em um texto completamente ilegível, sendo possível realizar a “descriptografia”, ou seja, o processo inverso para recuperar o conteúdo (SINGH, 1999). Segundo Stallings (2014), na criptografia existem duas áreas principais: i) os protocolos e os algoritmos de criptografia que possuem ampla gama de aplicações; e ii) segurança de rede e de Internet, que se baseia de forma expressiva em técnicas de criptografia.

Ainda, segundo Sousa; Moreira e Machado (2010) diversas empresas estão migrando o armazenamento de seus dados para a nuvem computacional, visto que buscam disponibilidade e agilidade em seus negócios. Essa tendência do armazenamento vem ganhando espaço em diversos ambientes, aumentando consideravelmente o volume de dados em repositórios, por esse motivo lança um novo olhar de importância para as chaves criptográficas com finalidade de assegurar que informações sejam acessadas, vazadas ou modificadas por outros usuários. Desta maneira, os algoritmos e protocolos utilizados, podem ser divididos em: i) criptografia simétrica; ii) criptografia assimétrica; iii) algoritmos de integridade de dados; iv) protocolos de autenticação (STALLINGS, 2014).

Na sistemática da criptografia simétrica, a mensagem criptografada é descriptografada com a mesma chave, ou seja, nas palavras de Carlos Maziero (2019,

p. 353) “se usarmos uma chave k para cifrar um texto, teremos que usar a mesma chave k para decifrá-lo”. O autor ainda ressalta que estes criptossistemas simétricos são muito eficientes para a cifragem de grande volume de dados, seja através de arquivos em disco rígido ou por uma conexão de rede.

Nestes casos, se a informação cifrada tiver de ser enviada à outro usuário, a “chave criptográfica secreta terá de ser transmitida a ele através de algum meio seguro”, podendo incorrer no incidente de “problema de distribuição das chaves”. (MAZIERO, 2019).

Por sua vez, o criptossistema assimétrico se caracterizam pela existência de duas chaves distintas: chave pública e chave privada. Neste ponto, Maziero (2019, p. 360) afirma que “uma informação cifrada com uma determinada chave pública só poderá ser decifrada através da chave privada correspondente, e vice-versa.”

Diferentemente da anterior, o cifrador assimétrico é indicado para pequenas quantidades de dados, uma vez que não suporta grande volume de dados. Além dessas características, exemplifica a diferença entre os cifradores simétricos e assimétricos, conforme abaixo:

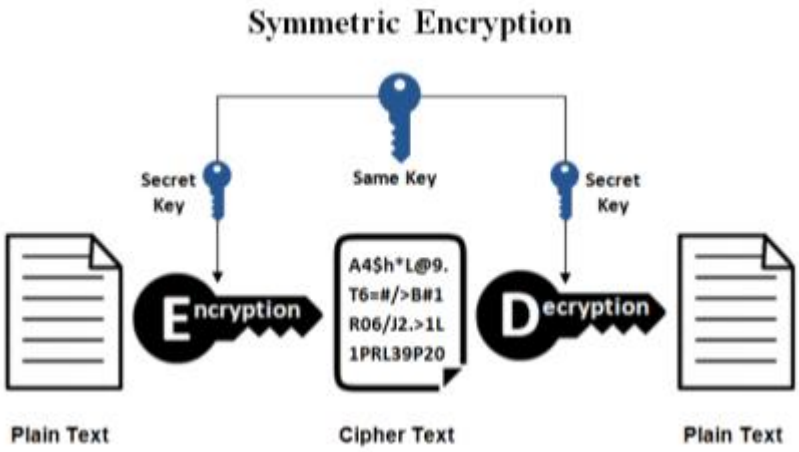

Figura 02: Representação de criptografia simétrica (Fonte: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences)

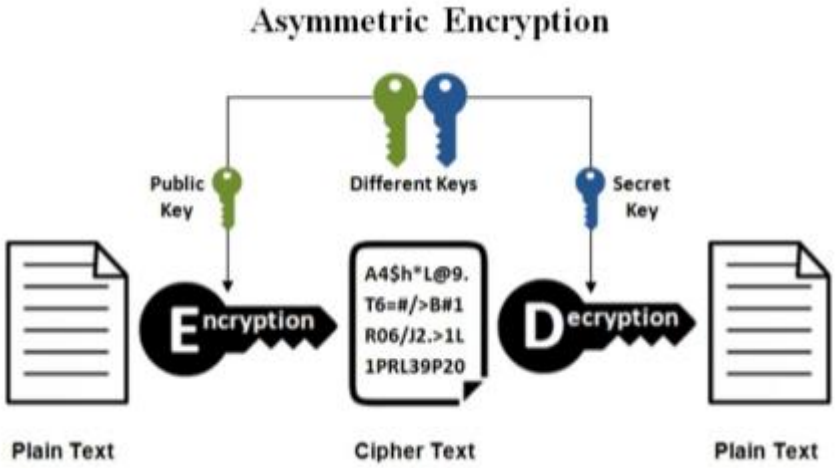

Figura 03: Representação de criptografia assimétrica (Fonte: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences)

No que diz respeito ao algoritmo de integridade de dados, ele é basicamente representado por um código denominado "*hash criptográfico*". Para garantir a integridade do dado, o *hash* é gerado por um algoritmo de dispersão, capaz de identificar um arquivo ou informação de forma necessariamente exclusiva (RIBEIRO; HIRA; ZUFFO,2006).

Por fim, no caso dos protocolos de autenticação dois aspectos estão envolvidos: assegurar a autenticidade das partes e assegurar que a comunicação não sofra interferências, a ponto de sofrer alterações ou intromissões desautorizadas. (PEREIRA. GUEDES; ASSIS, 2015).

Não menos importante, a ferramenta de *framework* de segurança cibernética NIST (*NIST Ciber Security Framework*) é comumente utilizada para auxiliar organizações. Luís Almagro (2019, p.02), secretário-geral da Organização dos Estados Americanos (OEA), afirma que o framework identifica "as normas e diretrizes de segurança aplicáveis em todos os setores e infraestrutura crítica, dando uma abordagem flexível e repetível", voltada a prevenção, detecção e resposta de ameaças cibernéticas e ataques cibernéticos.

Existem várias definições para *framework*s. Uma delas consiste em dizer que "um *framework* pode ser visto como gerador de aplicações desde que seja planejado para ser usado como base para o desenvolvimento e várias aplicações dentro de um determinado domínio" (MATTSSON, 1996). Dessa forma, o *framework* atua como referência para o alcance da segurança a partir do conjunto de atividades necessárias: identificação, proteção, detecção, resposta e recuperação das atividades, além de

auxiliar no processo de gestão da segurança da informação ao organizar e elencar os riscos, as atividades e as ameaças.

Guilherme Teles (2020) afirmou que apesar do alto custo de implementação, o NIST vem se tornando o *framework* de segurança com maior adesão no mundo pelas Organizações, inclusive dentro do Brasil. Dividido em categorias e subcategorias, as funções do NIST são alinhadas ao perfil exclusivo de cada organização, atreladas ao objetivo e realidade prática, baseando-se em: identificar, proteger, detectar, responder e recuperar recursos e serviços. É nesse sentido que o *framework* se torna uma das ferramentas práticas mais utilizadas, pois traça um plano de ação para manutenção dessas práticas, conferindo mais segurança (WADLOW, 2000).

Dentre os instrumentos apontados que compõem o conjunto de segurança, em um processo à parte, algumas medidas de certificação desses sistemas operacionais estão relacionadas a segurança física do ambiente (HINTZBERGEN, et.al, 2018). Medidas organizacionais, estruturais e eletrônicas constam como as principais para mitigar invasões e exposições de risco sem necessidade, portanto, câmeras de segurança, controles de entrada, sensores de presença ou quebra de vidro, contatos magnéticos e etc., podem ser consideradas barreiras físicas de segurança organizacional. Além da vigilância, o objetivo da segurança física também é o de manutenção, visando manter equipamentos que operam íntegros, sem avarias, uma vez que essa hipótese pode comprometer diretamente os servidores que congregam a segurança física.

Conforme estabelecido na LGPD (artigos 40, 41, 42 e 43) as medidas de boas práticas envolvem um sistema amplo e complexo de relações e previsões como a instituição de mecanismos de educação e prevenção em face da segurança da informação, atuação de organismos de certificação e treinamento de equipes junto à atuação das autoridades supervisoras (BRASIL, 2018).

A união de ferramentas operacionais e físicas de segurança como método de barreira aos ataques e ameaças, podem auferir maior grau de desempenho na segurança dos sistemas de armazenamento de dados das organizações e instituições, além de elevar a confiabilidade perante o mercado.

A necessidade de segurança é um fator que vem transcendendo o limite da produtividade e da funcionalidade, pois, enquanto a velocidade dos processos de negócios significa vantagem na produtividade, a falta de segurança pode resultar em

grandes prejuízos, alguns até irreparáveis, se não observados os critérios elementares para a proteção dos sistemas e de suas bases de dados.

CAPÍTULO II – O CICLO DE VIDA DE DADOS SENSÍVEIS EM SOFTWARE DA SAÚDE DO BRASIL

O presente capítulo elenca os sistemas mais comuns utilizados pela área da saúde, em especial pelos planos de saúde suplementar, e verifica como esses sistemas funcionam por meio de tecnologia interoperável, considerando a problemática de compartilhamento de dados pessoais e sensíveis. Nesse estudo foi possível identificar quais dados cada sistema armazena e compartilha com demais na ordem de comunicação e gerenciamento informacional.

O traço de evidência refere-se aos dados coletados pelo Padrão de Troca de Informação na Saúde Suplementar (TISS), utilizado para gestão administrativa dos planos de saúde privado que atuam na manutenção da tríade: operadoras, prestadoras de serviços e beneficiário.

Assim busca-se averiguar, mediante comparação com o sistema HL7 de padrão internacional, como o TISS realiza a troca de dados e qual seria o grau de confidencialidade no trânsito e armazenamento desses dados

Levando em consideração a Lei Geral de Proteção de Dados Pessoais e a Segurança da Informação, o confronto dessas tecnologias utilizadas para cada sistema se concentra em esmiuçar 02 (dois) aspectos principais: (i) a garantia de privacidade e sigilo das informações cedidas pelos titulares de dados e (ii) as evidentes vulnerabilidades no compartilhamento de dados através da troca de informações entre sistemas interoperáveis.

2.1. A implementação de sistemas padrões na saúde suplementar e o ciclo de vida dos dados pessoais sensíveis que alimentam suas bases de dados

A Agência Nacional de Saúde Suplementar (ANS), desde sua criação em 2000 (BRASIL, 2000), vem publicando inúmeras resoluções normativas com o objetivo de conhecer e organizar melhor o mercado de saúde suplementar de acordo com o surgimento de novas necessidades.

O estabelecimento de regras de funcionamento das operadoras, reservas técnicas, gerenciamento de contas, registros de produtos para comercialização, requerimentos de informações junto às operadoras, etc., fazem parte desse processo de edificação da ANS (BRASIL, 2000).

Essa grande quantidade de resoluções busca equilibrar o funcionamento das funções que envolvem todos os atores dessa relação: operadoras, prestadores de serviço e os beneficiários de planos de saúde.

Destaca-se que os dados pessoais e dados pessoais sensíveis que alimentam as bases de dados de uma determinada organização, empresa ou instituição, obedecem a um “ciclo de vida”. Esse ciclo corresponde em um caminho pelo qual os dados percorrem o ambiente organizacional, desde o momento da sua coleta até sua exclusão.

Contudo, o caminho percorrido pelo ciclo de vida converge para confirmar que a manifestação da vontade do titular de dados foi – aqui o paciente de determinada clínica médica ou hospitalar – inequívoca, informada e transparente (art. 8º da LGPD) (BRASIL, 2018).

Cabe explanar que ao se referir a dados relacionados à saúde, estes são, em sua maioria, dados com características alfanuméricas que possuem informação verificada a partir do no uso de padrões de linguagem pelos profissionais da categoria.

O tema da padronização de informações em sistemas de saúde ainda é um debate bastante recente na agenda técnica e política da Agência Nacional de Saúde Suplementar (ANS). Os sistemas de coleta de informação do mercado desenvolvidos pela ANS permitiram observar a falta de padronização de conceitos e estruturas das informações, o que comprovadamente dificulta em demasiado a análise do paciente pelo profissional e a estruturação de modo mais abrangente de todo o setor.

A Associação de Medicina de Grupo do Estado de São Paulo (ABRAMGE-SP) e a Associação dos Hospitais do Estado de São Paulo (AHESP), em meados de 1992, iniciaram um estudo piloto sobre padronização e codificação de procedimentos e serviços hospitalares. O objetivo da ação era essencialmente sanar as dificuldades administrativas decorrentes da grande diversidade de guias, impressos de encaminhamento, atendimento aos beneficiários, prestação de contas, facilitando assim a adoção de sistema padrão de transmissão eletrônica de dados.

Na busca pela padronização de nomenclaturas, suporte técnico, indicações clínicas e demais registros, foram levantados os principais sistemas que são utilizados como ferramentas de suporte para o cuidado em saúde e enfermagem. Destacam-se os principais: SNOMED CT; HL7; TISS e o NMDS, que se encontram desenvolvidos na sequência.

Além disso, a tecnologia inserida na maioria dos sistemas mencionados, envolvem a interoperabilidade que permite que seja possível diminuir a fragmentação, aumentar a qualidade de dados clínicos, tornando os sistemas mais homogêneos (RAY, 2014).

Inicialmente, o *Systematized Nomenclature of Medicine – Clinical Terms*[23] (SNOMED-CT) é considerado destaque na área da saúde. A primeira versão da SNOMED foi lançada em 1974 e, desde então, as versões foram atualizadas e publicadas, entre elas: SNOMED versão 3.5 em 1998; SNOMED – RT em 2000; e, em 2002 o SNOMED tornou-se SNOMED – CT, resultado da fusão entre SNOMED – RT com o *Clinical Terms* na terceira versão da *National Health Service*[24] (NHS) do Reino Unido.

O desenvolvimento da SNOMED – CT envolveu grandes grupos de profissionais especializados na área da saúde para desenvolver terminologias axiais que padronizassem o vocabulário médico com o objetivo de indexar o conjunto de registros médicos, incluindo dados vinculados aos sinais de sintomas, diagnósticos e procedimentos, abrangendo a maior parte das necessidades de documentação/registro de saúde.

Esse padrão de dados permite uma ampla integração entre os dados de saúde relacionados a determinado paciente, armazenadas em registro médico eletrônico dentro de uma estrutura única de dados (BARRA; SASSO, 2012).

A precisão na representação dessas informações na área da saúde, facilita a estruturação e a interoperabilidade entre os sistemas de informação, permitindo a codificação, o armazenamento, a troca e a agregação dos dados clínicos.

Na mesma toada sobre sistema com base de dados agregada, o *Hight Level 7* (HL7), além de norma, é também o nome de uma organização certificada pela *American National Standards Institute* (ANSI), fundada em 1987, voluntária e sem fins lucrativos, que desenvolve normas, especificações, protocolos ou padrões que devem ser utilizados na troca de dados clínicos e administrativos em Sistemas da Informação (SI).

O padrão HL7 é produzido pela *Hight Level Seven International*, e é formado por um conjunto de padrões internacionais para a transferência de dados clínicos e

---

[23] Tradução: Nomenclatura Sistematizada da Medicina – Termos Clínicos
[24] Tradução: Sistema Nacional de Saúde

administrativos entre aplicações de software utilizada por diferentes profissionais de saúde.

A referência alfanumérica 7 (sete), para John D. Day e Hubert Zimmermann (2014) diz respeito aos padrões da última camada do modelo *Open System Interconnection*[25] (OSI), ou seja, a sétima camada de aplicação onde se definem propriamente ditos as mensagens e os mecanismos de troca de dados. Diogo Lajas (2017) aponta que os principais objetivos do HL7 são:

1) ser o mais abrangente possível;

2) ser flexível;

3) norma aberta;

4) fornecer formatos e protocolos na comunicação entre aplicações;

5) permitir a integração de diversas aplicações num SI;

6) fornecer um meio para atingir a interoperabilidade;

7) com a integração dos dados, é capaz de melhorar o processo de decisão clínica;

8) possuir *workflows* otimizados;

9) reduzir conflitos e problemas de comunicação na transmissão de mensagens.

Esse modelo de padronização se destina a permitir que as organizações de saúde compartilhem facilmente dados clínicos e administrativos, minimizando a desfragmentação de cuidados médicos diante de barreiras geográficas, ou seja, mantém a integridade da informação independentemente da localização do paciente.

Para demonstrar o funcionamento, Lajas (2017) apontou o seguinte exemplo: existe uma nova requisição de análises ao laboratório, em seguida é enviada uma mensagem HL7 do tipo “OML”[26] (pedido ao laboratório) com as informações necessárias para que a aplicação do departamento de análises laboratoriais possa proceder a análise requerida. Ao receber e processar a mensagem enviada desse SI central, a aplicação do departamento de análises laboratoriais envia uma mensagem

---

[25] Open System Interconnection (OSI): para facilitar o processo de interconectividade entre máquinas de diferentes fabricantes, a Organização Internacional de Padronização (ISSO – International Standards Organization) aprovou, no início dos anos 80, um modelo de referência para permitir a comunicação entre máquinas heterogêneas, denominado OSI (Open System Interconnection). Esse modelo serve como base para qualquer tipo de rede, seja de curta, média ou longa distância.

[26] Laboratory Order Message (OML).

do tipo “ACK”[27] (confirmação de recepção) para outro SI central. Ou seja, sempre que há um evento em SI que necessite informar, requisitar informação ou serviço de outro SI, haverá troca de mensagens HL7 entre estes SI (LAJAS, 2017).

O conjunto de tarefas exercida pelo HL7 (admissão, transferência, alta, pedidos laboratório, pedidos radiologia, gestão de ordem, finanças, observação, etc.) circula entre as diversas integrações presentes nas instituições de saúde. Desse modo, cada segmento que compõe a mensagem HL7, tem a sua própria estrutura constituída por vários campos e subcampos, havendo variação nos eventos. Em suma, o HL7 especifica os tipos de mensagens trocadas entre aplicações instaladas nos diversos departamentos hospitalares, o formato de dados, a sua representação, dentre outros, e a sua estrutura de mensagem pode variar de acordo com o evento.

A Figura 04 representa um esquema de como é construída uma mensagem genérica de HL7.

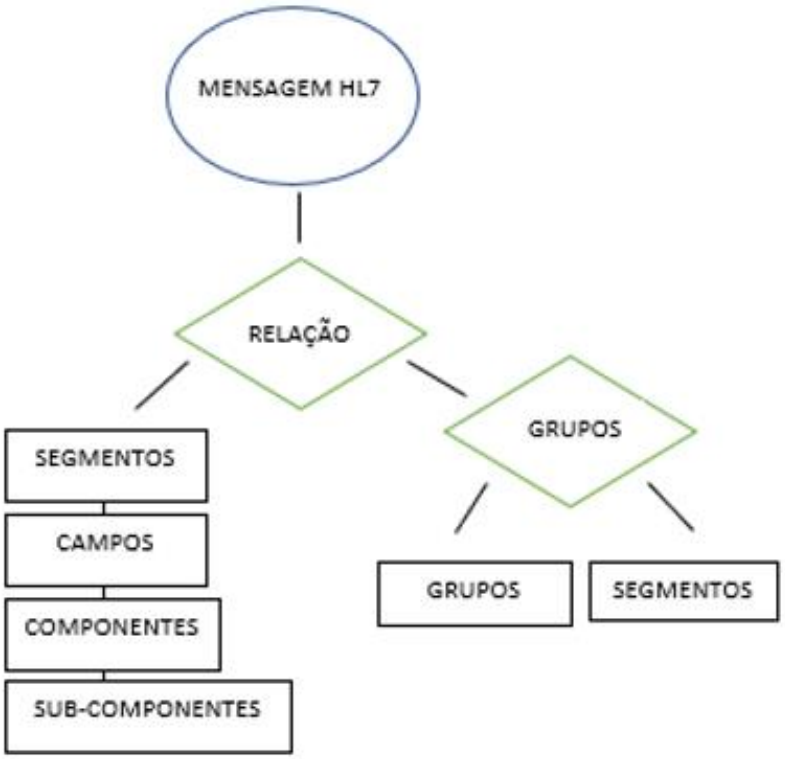

Figura 04: Modelo de construção de mensagem genérica no HL7. Fonte: Adaptado de (CRUZ, 2015).

Disponível em diferentes versões (versão 2, versão 3, CDA e FHIR), o HL7 versão 3 é a mais atual, orientada pelo *Hight Definition Framework* (HDF) capaz de

---

[27] General Acknowledgment Message (ACK).

cobrir dados relacionados a mensagens, documentos clínicos, processos, ferramentas, sujeitos, regras e outros artefatos relevantes para o desenvolvimento e melhoria no atendimento médico.[28]

Segundo Bender e Sartipi (2013), o FHIR é a última e mais atualizada versão do HL7 até o momento e trouxe uma nova abordagem para a troca de informações em saúde. Baseado na arquitetura *Restfull*[29] (FIELDING,2000) se tornou um padrão robusto evitando a utilização de ferramentas complexas. Já para Franz (2015), abordagens baseadas em FHIR tem gerado preocupações relacionadas com a segurança a fim de garantir a autenticidade, autorização e a autoridade das informações.

Voltados às versões de sistema nacional, no Brasil, a ANS instituiu o Padrão TISS (Troca de Informações na Saúde Suplementar), para definição de um padrão para a troca de informações sobre o atendimento disponibilizado aos beneficiários, entre operadoras de planos privados e prestadores de serviço (BRASIL, 2012).

Inspirado no formato do HL7, o Padrão TISS tem o objetivo de atingir a compatibilidade e interoperabilidade funcional e semântica entre os diversos sistemas independentes para fins e avaliação de assistência à saúde (caráter clínico, epidemiológico ou administrativo) e seus resultados, orientando o planejamento do setor.

Cerca de mil e quinhentas unidades foram registradas na ANS e, aproximadamente, duzentos mil prestadores de serviços foram certificados para a realização de eventos de assistência prestados aos beneficiários (DIAS, 2011).

O último padrão utilizado na saúde é essencialmente destinado à área de enfermagem: *Nursing Minimum Data Set*[30] (NMDS). Esse padrão representa a primeira tentativa de padronizar os dados essenciais e uniformes para a prática da Enfermagem. O NMDS é derivado do conceito de *Uniform Minimum Health Data Set*[31]

---

[28] Disponível em: https://interopera.esy.es/principais-padroes-e-metodologias-hl7/

[29] O “RESTfull” é a aplicação de maneira desenvolvida de “REST” que é um termo definido para “Trasferência de Estado Representacional” (*Representational State Transfer*). Criado em 2000 por Roy Fielding em sua tese de doutorado no qual ele descreve sobre um estilo de arquitetura de software sobre um sistema operado em rede. Portanto, os *webservices* que estão em conformidade com o estilo de arquitetura “REST”, são denominados de web services “RESTfull”.

[30] Tradução livre: Conjunto de Dados Mínimos em Enfermagem

[31] Tradução livre: Conjunto de Dados Mínimos Uniformes em Saúde

(UMHDS) estabelecido em 1983 pelo *Health Information Policy Council* [32] do *U.S. Departement of Health and Human Services*[33].

Esse padrão de dados é conceituado como um conjunto mínimo de elementos de informação, com definições e categorias uniformes específicos da área de enfermagem, que satisfaz a necessidade de informação dos usuários de dados múltiplos no sistema de atenção à saúde. O NMDS apresenta-se para as seguintes funcionalidades:

a) permitir a comparação das atividades de Enfermagem dos distintos cenários de cuidado, populações clínicas, zonas geográficas e tempos;

b) descrever o cuidado de Enfermagem dos pacientes e seus familiares em uma variedade de ambientes, tanto institucionais, como não institucionais;

c) demonstrar ou projetas as tendências observadas na prestação do cuidado de Enfermagem e os recursos de Enfermagem designados aos pacientes conforme seus problemas de saúde e os diagnósticos de Enfermagem;

d) incentivar as investigações (pesquisas) de Enfermagem utilizando os vínculos com os dados detalhados existentes nos sistemas de Enfermagem e outros sistemas de informação sanitária e;

e) proporcionar dados sobre cuidado de Enfermagem para facilitar e influenciar sobre a adoção de decisões em relação às políticas clínicas, administrativas e sanitárias.

O NMDS compreende dezesseis elementos divididos em 03 (três) categorias amplas e integradas, classificadas como: a) 4 (quatro) elementos de cuidado de Enfermagem: diagnóstico , intervenção, resultados, e intensidade de cuidado de Enfermagem; b) 5 (cinco) elementos de identificação do paciente: nome, data de nascimento, sexo, raça e etnia, residência; e, c) 7 (sete) elementos do serviço: número da agência do serviço de saúde, número de registro único de saúde do paciente, número de registro único do profissional de Enfermagem que prestou o cuidado, data da admissão, data de alta, dados de encaminhamento do paciente e dados sobre o tipo de pagamento de serviço prestado.

Todas as terminologias utilizadas mundialmente pela área de enfermagem estão diretamente vinculadas aos padrões do NMDS (BARRA; SASSO, 2011), o que

---

[32]Tradução livre: Conselho de Políticas de Informação em Saúde
[33] Tradução livre: Departamento de Saúde e Serviços Humanos dos Estados Unidos

confirma que a padronização de sistemas é fundamental para a construção do cuidado em saúde, propiciando a promoção de condições que determinam uma boa contribuição para o paciente e para a sociedade.

Essas explicações visam fundamentar que a implementação de padrões e a utilização de sistemas para o armazenamento de dados, colaboram para a fluidez do serviço na área da saúde. Isso porque a contribuição se estende para além do processo de gestão de dados e informações de pacientes em ambientes clínicos e hospitalares, mas também possibilita uma entrega assistencial colaborativa pelos profissionais, com melhor desempenho da análise clínica, rompendo barreiras físicas de acesso, e possibilitando a integração do paciente com todo o ciclo empresarial.

Até aqui foram apresentadas possíveis soluções para maior agilidade profissional e simplificação do preenchimento de registros eletrônicos em saúde, a partir dos critérios de padronização, além do maior gerenciamento e abordagem precisa de informações de pacientes alcançado através do compartilhamento de sistemas interoperáveis.

Resta ainda saber como são armazenados os registros eletrônicos desses sistemas hospitalares e clínicos. Conforme consta no início do item 1.3 do Capítulo 1, o Ministério da Saúde define no Capítulo II da Portaria nº2.073, de 31 de agosto de 2011, o modelo de referência *OpenEHR* para o Registro Eletrônico de Saúde (RES) define o Padrão TISS para a interoperabilidade entre sistemas na saúde suplementar (BRASIL, 2011).

Os softwares que seguem o padrão *OpenEHR* são considerados abertos, adaptáveis e colaborativos, pois se baseiam em modelos de informação padronizados e em código aberto (ALQASSIM et. al., 2016).

Para os registros eletrônicos na área da saúde, Jesús N. S. Rubí (2016, p.18) sugere que o armazenamento seja realizado em nuvem, o que facilitaria o "crescimento das plataformas interoperáveis em saúde (HIE, do inglês, *Health Information Exchange*), possibilitando uma sensível redução de custos e um aumento significativo de facilidades para a Cadeia Assistencial".

A *cloud computing* [34] é definida pelo *National Institute of Standards and Technology* (NIST) como um modelo que permite o acesso à rede sob demanda a um

---

[34] Tradução livre: computação em nuvem

conjunto compartilhado de recursos de computação configuráveis que pode ser rapidamente provisionado autorizando e lançado informações com o mínimo de esforço de gestão ou a interação de um prestador de serviço (MELL;GRANCE, 2012).

Ainda segundo o NIST, o modelo de computação em nuvem (*cloud computing)* está composto por elementos essenciais demonstrados na Figura 03, sendo eles: característica essenciais: amplo acesso à rede, rápida elasticidade, serviços otimizados e autosserviço por demanda, modelos e serviço: administradores de sistemas, desenvolvedores e usuários finais; e modelos de desenvolvimento: nuvem pública, nuvem privada, nuvem comunitária ou nuvem híbrida (MELL;GRANCE, 2012).

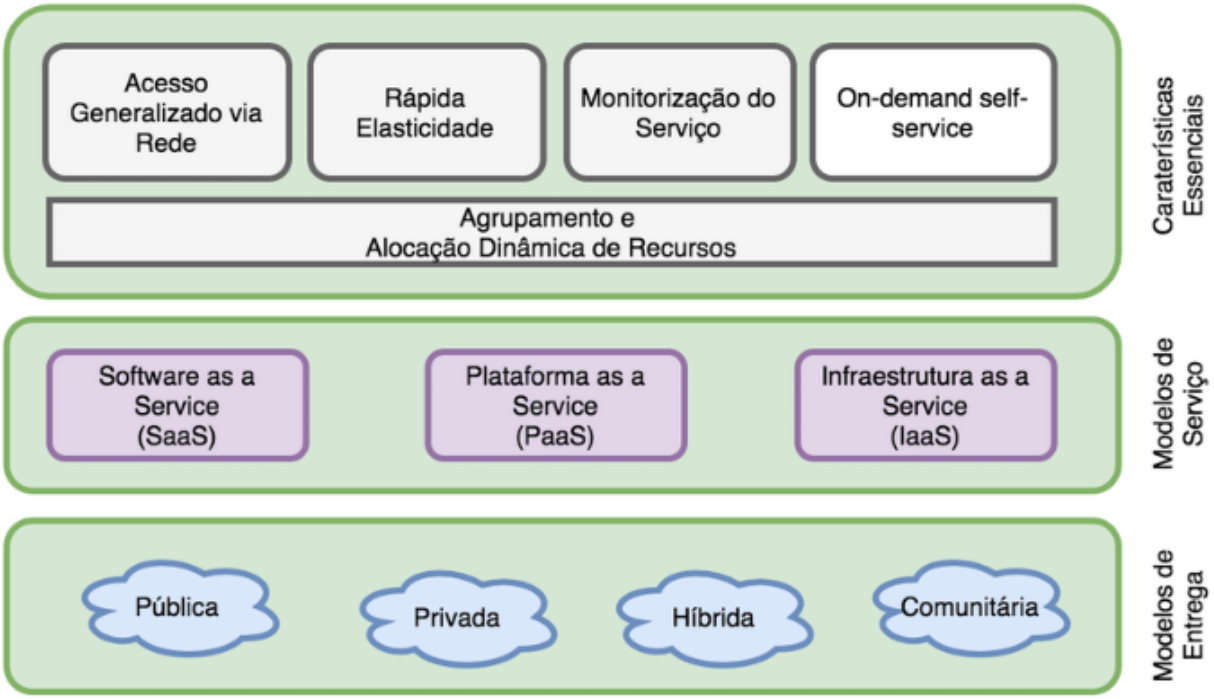

Figura 05: Definição de funcionamento de computação em nuvem. Fonte: (BIOCO, 2016)

Neste caso, as amplas possibilidades que demonstram caracterizado o sistema de armazenamento em nuvem da Figura 05 confirmam que este modelo oferece várias vantagens sobre os modelos tradicionais de *software* local, sendo as principais: menor custo de implantação, melhor agrupamento de recursos, otimização de serviços, amplo acesso à rede e a base de dados, além de outras funcionalidades (RUBÍ,2016).

Assim, é possível concluir que a utilização do modelo de referência *OpenEHR,* torna possível que o armazenamento de dados utilizados para o preenchimento do

RES seja realizado por meio do modelo de *cloud computing*, uma vez que otimiza não apenas o armazenamento desses dados, mas também as facilidades que o acesso lhe proporciona, resguardadas as barreiras de acesso e segurança para melhor utilização e fluidez na prestação do serviço pelos profissionais de saúde.

2.2. As características do sistema do Padrão TISS adotado na saúde suplementar do Brasil

Quando o tema é sistema computacionais voltados à área da saúde, Médici (2010) afirma que tendem a ser “naturalmente fragmentados”. No entanto, a introdução de sistemas de registros e organização de informações passaram a ser um atrativo para os agentes do setor, podendo trazer benefícios ou não. Segundo o autor, no final da década de 1960 começaram a surgir as primeiras formas de informatização dos serviços de saúde, ainda rudimentares e com dificuldades para “organizar e cruzar informações existentes sem o devido foco nos pacientes e usuários” (MÉDICI,2010). O cenário começou a mudar a partir da década de 1980 e essa realidade passou a conviver com o surgimento de novas tecnologias que, para Médici (2010), voltadas ao gerenciamento “em saúde como os grupos relacionados de diagnóstico (DRGs), a digitalização de fichas clínicas e o cruzamento dessas informações com dados cadastrais dos usuários dos sistemas de saúde”.

Portanto, atrelado aos sistemas de melhoramento e gerenciamento de saúde estará sempre ligado o Registro Eletrônico em Saúde que, para a norma ISO/TR 20514 e ISO/TS 18308 é definido como um “repositório de informação a respeito da saúde de indivíduos, numa forma processável eletronicamente” (ISO/TR,2005; ISO/TS,2004).

Sob a influência do aperfeiçoamento em sistemas informáticos utilizados na saúde, a Lei nº 9.961 de 2000 (BRASIL, 2000) foi criada e concedido à Agência Nacional e Saúde Suplementar (ANS) as atribuições de regulação do setor de saúde privada.

Nos dispositivos legais há expressa menção sobre a competência, estrutura organizacional, constituição de patrimônio, receitas financeiras, etc. Especialmente no art. 3º da legislação, há definição sobre a finalidade institucional da ANS, assim descrita: “promover a defesa do interesse público na assistência suplementar à saúde, regular as operadoras setoriais e contribuir para o desenvolvimento das ações de saúde do país” (BRASIL, 2000).

A dinâmica de funcionamento e o modelo assistencial da saúde suplementar, no entanto, são definidos pela Lei nº 9.656 de 1988 (BRASIL, 1998). Segundo o Plano Diretor de Tecnologia da Informação e Comunicação 2020-2021 (ANS, 2020 p. 10), existem atualmente no Brasil cerca de mil cento e cinquenta operadoras que oferecem assistência à saúde, ficando a encargo da ANS o acompanhamento e fiscalização das atividades assistenciais e de gestão, de forma a garantir o interesse público e a qualidade do atendimento realizado.

Mesmo com o intenso relacionamento entre as operadoras e os prestadores de serviço em saúde, havia pouco investimento em Tecnologia da Informação (TI) com capacidade para facilitar a complexidade envolvida no intercâmbio de dados. E foi a partir desse desafio no cenário, que ANS deu início a elaboração de uma norma nacional utilizada para a troca de informações em saúde, intitulada como Padrão TISS (Troca de Informação em Saúde Suplementar) (MENDES et. al, 2009).

O trabalho de pesquisa e desenvolvimento dessa regulamentação teve início em maio de 2003, a partir do convênio com o Banco Interamericano de Desenvolvimento (BID) (ANS, 2006).

Com o objetivo de utilizar denominações padrões no âmbito da saúde e facilitar o intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde, a ANS ainda propôs o Padrão TISS para a redução das queixas de volume de formulários a serem preenchidos, os burocráticos procedimentos para a obtenção de autorizações e liberações, ocorrência de fraudes, impossibilidade de comparação de dados de saúde do paciente, dentre outras consequências da setorização (ANS, 2006).

Para isso, a ANS organizou um grupo de trabalho interno que analisou os padrões de informações já trocados no mercado, com o objetivo de propor um modelo unificado de troca de informações em saúde suplementar (ANS, 2006).

Na intenção de harmonizar a relação entre operadoras e prestadores de serviço, reduzir custos administrativos referentes ao processo de faturamento, aprimorar a qualidade das informações trocadas e, sobretudo, agilizar o atendimento do beneficiário de planos de saúde, a ANS publicou em 26 de outubro de 2005 a Resolução Normativa nº114 (ANS, 2005), posteriormente atualizada pela Resolução Normativa nº153 (ANS, 2007), que estabelece o padrão eletrônico obrigatório para a Troca de Informações em Saúde Suplementar (TISS) a ser utilizado pelas operadoras e prestadores de serviço a respeito dos eventos de saúde realizados em favor do

beneficiário, considerada um grande marco na discussão sobre padrões em saúde no país.

A Resolução Normativa nº114 (ANS, 2005) estabelece a obrigatoriedade de adoção do Padrão por todas as operadoras e seus prestadores de serviços contratados/conveniados.

O Padrão TISS foi desenvolvido seguindo a estrutura do Comitê ISO/TC215 *Health Informatics* que aprova a implementação de padrões para informática em saúde e divide em cinco componentes essenciais para o fundamento representados na Figura 06.

Figura 06: Componentes do Padrão TISS. Fonte: (ANS, 2021)

Inicialmente, o componente organizacional[35] estabelece o conjunto de regras operacionais que servirão de embasamento para as medidas adotadas ao longo de implementação e utilização do *software* (ANS,2012). Em seguida, o componente de conteúdo e estrutura[36] compreende a arquitetura dos dados utilizados nas mensagens eletrônicas e no plano de contingência para a coleta e disponibilidade dos dados de atenção à saúde (ANS,2014). Essa padronização incorporou as guias de consulta, exames, internações e tratamento odontológico. Além disso, os prestadores de serviço incitaram a necessidade de incorporação de outra demanda: padronização dos demonstrativos de pagamento, ou seja, documentos a serem enviados pelas operadoras que descrevem os serviços pagos e não pagos (glosas), com uso de códigos padronizados (DIAS, 2006).

---

[35] http://guia.serpram.com.br/portaltiss/InstrucoesTiss/DOCTISS30_01.pdf

[36] http://www.cafazonline.org.br:8181/portal/credenciado/arquivos/Padrao_TISS_Componente_Conteudo_Estrutura_201405.pdf

Na sequência, o componente de representação de conceitos[37] em saúde determina o conjunto de termos para identificar os eventos e itens assistenciais na saúde suplementar, consolidados na Terminologia Unificada da Saúde Suplementar (TUSS) (ANS, 2021).

Aqui os dados clínicos possuem representação a partir de código e nomenclatura gerados para a troca de informações entre as operadoras de plano privado de assistência a saúde e os prestadores de serviço de saúde sobre os eventos assistências realizadas em seus beneficiários (ANS,2021).

O componente da comunicação do Padrão TISS institui os meios e métodos de comunicação das mensagens eletrônicas definidas no componente de conteúdo e estrutura (ANS,). Esse modelo ainda compreende a autenticidade e qualidade de entrega dos dados. Assim, agrupam-se no padrão de comunicação que dizem respeito às mensagens eletrônicas projetadas a partir das guias padronizadas, e estruturas em XML[38].

Por fim, o componente da “segurança e privacidade” dedica-se a assegurar o direito individual ao sigilo, à privacidade, e à confidencialidade dos dados de atenção à saúde, com expressa determinação de cumprimento da legislação que versa especificamente sobre a privacidade (ANS,2017). Foi recomendado, pelo mesmo instrumento legal, que o componente de segurança e privacidade para a troca da informação na saúde suplementar seguisse o modelo do “Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico de Saúde (RES)” elaborado em conjunto com a Sociedade Brasileira de Informática em Saúde (SBIS, 2010) e o Conselho Federal de Medicina (CFM, 2010) (ANS,2017).

Inerente ao bom desenvolvimento do sistema, além do formato padrão de linguagem XML, a troca de documentos dinâmica entre empresas adotado pelo Padrão TISS é representado pela sigla EDI (*Eletronic Data Intercharge*). Conceitualmente o EDI é considerado “uma rede de acesso aos clientes do provedor, permitindo a conexão entre os sistemas eletrônicos de informação entre empresas,

---

[37] https://www.unimedara.com.br/Content/themes/TISS/Tabelas/TUSS%20-%20Demais%20terminologias%20-%20VERS%C3%83O%20202104.pdf

[38] XML é a sigla para “*eXtensible Markuo Language*”, cuja a tradução livre significa “linguagem de marcação extensível”. O XML possui origem na SGML (Standard Generalized Markup Language), um padrão especificado pela ISO 8879 em 1986.

independentemente dos sistemas e procedimentos utilizados no interior de cada empresa" (PIZYSIEZNIG, 1997, p. 55).

A integração de todos esses módulos em um sistema é o que possibilita troca de mensagens uniformes e eficientes com diferentes linguagens, o que é definido por Silva (2004) como "interoperabilidade". Assim, sobre a interoperabilidade, o pesquisador do serviço de informática do Instituto do Coração (InCor) do Hospital das Clínicas de São Paulo, Ramon Alfredo Moreno (2016, p.01) afirma que:

> a interoperabilidade é essencial para que seja possível: (i) oferecer ao profissional de saúde e ao paciente uma visão holística de todo o histórico médico do paciente; (ii) auxiliar o profissional de saúde, ela automatização de procedimentos computacionais e; (iii) permitir que seja utilizado todo o arsenal computacional desenvolvido ao longo dos anos para o processamento de dados do paciente, gerando alertas, notificações e lembretes.

Dessa forma, a dinâmica de troca de mensagens do Padrão TISS é também atribuída a ferramenta tecnológica: *webservice*. O *webservice* provê uma maneira padrão de interoperabilidade entre aplicações cliente/servidor por meio do *Hypertext Transfer Protocol* (HTTP) e, juntamente com padrões XML específicos para a construção de serviços, favorece para que uma grande quantidade de aplicações desenvolvidas em plataformas, linguagens e *frameworks*[39] distintos possam trocar dados (MACHADO; FRANCO; BERTAGNOLLI, 2016, p. 184 e 185).

A utilização do *webservice* demonstra eficácia quando utilizada junto ao protocolo SOAP (*Simple Object Access Protocol*), uma vez que a linguagem utilizada por esse protocolo baseado em XML determina um formato para a troca de informações em ambiente distribuído (MACHADO; FRANCO; BERTAGNOLLI, 2016).

Moreno (2016, p.01) aponta diversos desafios que envolvem a interoperabilidade da comunicação entre sistemas, especialmente por alguns acabarem sobrepondo-se a outro, restando incerta sobre a utilização do sistema ideal. Ainda, afirma que uma das condições mais importantes da adoção da interoperabilidade é a segurança e confidencialidade de dados do paciente, isso porque, a exposição de dados nesse

---

[39] Frameworks: é uma arquitetura desenvolvida com o objetivo de atingir a máxima reutilização, representada como um conjunto de classes abstratas e concretas, com grande potencial de especialização (MATTSSON, 1996).

intercâmbio de sistemas pode tornar a segurança suscetível e comprometer a confiabilidade do paciente perante serviço clínico ou hospitalar.

Neste ponto, o Padrão TISS utiliza a Internet para o transporte de dados que é dada especificamente por meio de arquivo XML – que será explorado com minúcias no item 2.3 desse Capítulo, e também prevê mecanismos de segurança para assegurar a integridade do conteúdo, mediante o suporte de um *hashcode*[40], com o objetivo de garantir que no momento da transmissão o dado não sofra qualquer alteração do começo ao fim.

O *hash,* como visto no item 1.4 do Capítulo 1, atua como algoritmo matemático criptográfico capaz de “cifrar” o dado (arquivos, mídias, senhas, documentos, etc.) compactando-o em um conjunto alfanumérico fixo de caracteres, conforme representado esquema da Figura 07.

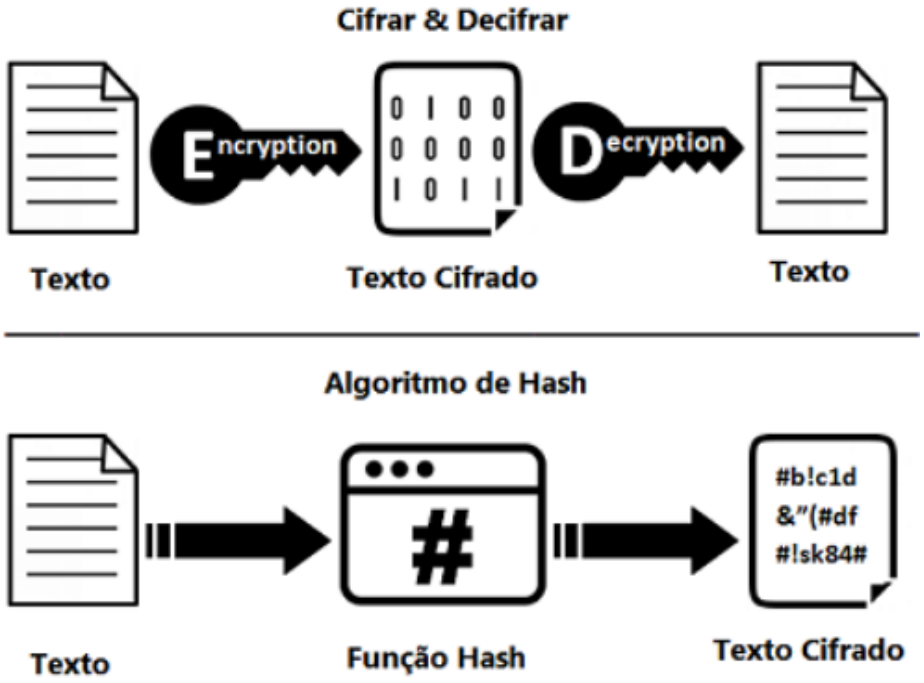

Figura 07: Funcionamento do *hash.* Fonte: http://www.macoratti.net/16/09/net_cripto2.htm

Seguindo a dinâmica da função *hash,* todas as informações de pacientes, resultado de exames clínicos, exames de imagens, protocolos de atendimento, dentre outras atividades que integram o atendimento à saúde, podem ser cifrados e transferidos à outro servidor de maneira compactada e com maior índice de

---

[40] Tradução livre: código *hash*

segurança, uma vez que seria “praticamente impossível” (SÁVIO, 2020) reverter o valor de um *hash* para identificar a mensagem original de entrada.

Assim, mesmo com a presença do componente de segurança que forma uma das bases de sustentação do Padrão TISS, a legislação nacional de proteção e governança de dados vigente segue sendo o horizonte na implementação de sistemas que admitem troca de informações.

Contudo, é inegável que as características da composição, transformam o dia a dia das empresas e dos profissionais de saúde na otimização de procedimentos de gestão, trazendo melhorias no atendimento e na prestação de serviço ao paciente.

2.3. Uma análise comparativa aos princípios da Segurança da Informação frente aos mecanismos de segurança adotados pelo TISS e HL7

O uso cada vez mais amplo e disseminado de sistemas informatizados para a realização das mais diversas atividades, como a integração com demais bases de dados por meio de redes de computadores, se mostrou um fator determinante na sociedade da informação.

Contudo, esse universo de conteúdos e contingentes digitais está sujeito a várias formas de ameaças, físicas e/ou virtuais que, como já visto, podem comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem a tríade: usuário, sistema e informação.

Considerando as importantes características de sistema apontadas nos protocolos TISS e HL7, estes foram os escolhidos para serem comparados no quesito estrutural de segurança no armazenamento e transferência de dados uma vez que possuem estrutura semelhante e são os mais utilizados pela saúde no Brasil (o Padrão TISS) e no mundo (Padrão HL7).

A segurança da qual se refere a abordagem deste tema, está especialmente ligada na Segurança da Informação (SI), já conceituada no item 1.4 do primeiro capítulo desta pesquisa, e seus princípios serão dissecados neste item para que possam servir de objeto de comparação aos protocolos.

Marciano e Lima-Marques (2006, p.94) afirmam que todas as proposições apontadas sobre a segurança da informação se baseiam ou derivam de conceitos de SI, além de atrelarem a SI como um domínio tecnológico em que ferramentas e

recursos são aplicados na busca por soluções de “problemas gerados, muitas vezes, com o concurso daquela mesma tecnologia”.

A correta gestão da Segurança da Informação é atingida com o compromisso de todos os usuários na aplicação das normas e procedimentos estabelecidos visando a padronização das ações de planejamento, implementação e avaliação das atividades voltadas à segurança (WILLIAMS, 2001). Estas diferentes atividades podem ser agrupadas conforme a seguinte disposição (ISACF,2001):

1) Desenvolvimento de políticas, com objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas;

2) Papéis e autoridades, assegurando que cada responsabilidade seja claramente entendida por todos;

3) Delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos;

4) Monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com a plena aderência à política, aos padrões e às práticas aceitáveis;

5) Vigilância, treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança.

Convém lembrar que a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) tem em seu site diversos documentos que abordam a necessidade de regulamentação adequada para a segurança da informação em seus aspectos gerais (OCDE, 2002, 1996), além de outros específicos voltados ao comércio eletrônico (OCDE, 2001a) e privacidade (OCDE, 2001b).

Ainda, aliada às atividades, os princípios que a OCDE apresenta também são compatíveis para o desenvolvimento de uma cultura de Segurança da Informação (OCDE, 2002), sejam eles:

i) vigilância;

ii) responsabilidade;

iii) participação;

iv) ética;

v) democracia;

vi) avaliação de risco;

vii) delineamento e implementação da segurança;

viii) gestão da segurança;

ix) reavaliação.

Observa-se que o cumprimento de tais princípios, para Marciano e Lima-Marques (2006, p.131) é uma atividade discricionária, de modo que a tomada de decisão dessas medidas encontra-se sob o poder de gestão dos administradores que podem aderir ou não à essas recomendações. Eventualmente, dentre as opções que se encontram para o cumprimento de padrões de segurança, algumas empresas optam por aderir à padrões internacionais, no entanto, diferentemente ao afirmado por Marciano e Lima-Marques (2006, p.131), essa decisão de aderir à influência de fóruns externos não enfraquece o cumprimento da legislação local.

É por este motivo que Pemble (2004) sugere que a Segurança da Informação deva ser definida nos termos das atribuições do profissional responsável por ela e que a utiliza. O autor ainda descreve 03 (três) esferas e atuação de tais profissionais em torno das quais a segurança deveria ser parametrizada e compreendida, sejam elas:

1) A esfera operacional, voltada ao impacto que os incidentes podem gerar à capacidade da organização de sustentar os processos do negócio;

2) A esfera da reputação, voltada ao impacto que os incidentes tem sobre o valor da “marca” ou sobre o valor acionário;

3) A esfera financeira, voltada aos custos em que se incorre na eventualidade algum incidente.

Dessa forma, o fenômeno da “segurança” comporta uma análise computacional interna e externa. Quando se trata sobre o assunto, Schneier (2001) afirma que a segurança pode ser facilmente confundida com a criptografia de computadores, enquanto Marciano e Lima-Marques (2006, p.92) entendem a criptografia apenas como um dos elementos para a segurança da informação.

Inclusive, ao que tange a criptografia, Marciano e Lima-Marques (2006, p.93) afirmam que a criptografia, junto com demais inovações tecnológicas “incorporam elementos que, se não forem devidamente analisados, podem resultar em impactos negativos que se contrapõem e até mesmo anulam os benefícios alcançados”, uma vez que associados podem causar falhas desconhecidas e agravar a situação de segurança.

Além da criptografia, a segurança computacional inclui ações de controle de computadores e privilégios de usuários, proteção contra cópia, proteção contra vírus, medição de *software* e segurança de banco de dados (SCHNEIER,2001).

Bruce Schneider (2001, p.131) afirma que existem inúmeros modelos teóricos para explicar segurança, a maioria deles são provenientes de sistemas militares custeados pelo Departamento de Defesa nas décadas de 1970 e 1980. Estes sistemas, com denominação de “segurança multinível” foram projetados para lidar com diversos níveis de classificação dentro de um sistema, o que justifica a denominação.

No quesito controle ou gerenciamento de usuários, é tarefa da TI realizar a verificação individual ou de grupos para permissões de acesso aos vários recursos tecnológicos da empresa como os sistemas dispositivos, aplicativos, sistemas de armazenamento, redes, serviços e etc. Assim, a segurança pode ser implementada de diversas formas a partir de permissões independentes e setorizadas, exemplo: leitura, escrita e execução (SCHNEIER,2001).

O elemento da segurança pode ser aplicável na setorização de autorizações para acesso ao armazenamento de dados em diferentes modelos de nuvens, quais sejam: pública, privada, comunitária ou híbrida (RUBÍ, 2016).

Rubí (2016, p.17) afirma que enquanto o modelo de computação em nuvem pública dispõe de uma infraestrutura ao público geral e pode permanecer nas instalações do fornecedor; o modelo de computação em nuvem privada, em contrapartida, é acessível somente a um grupo específico de pessoas autorizadas, podendo ser instalada dentro da própria empresa, o que lhe agrega diferencial no quesito da privacidade. Por sua vez, a nuvem comunitária permite uma infraestrutura compartilhada por uma comunidade de organizações com interesses em comum; já, o modelo de computação em nuvem híbrida congrega duas ou mais estruturas distintas (comunitária, privada ou pública) que permanecem dentro da empresa porém, através de tecnologias padronizadas, disponibilizam dados e possibilitam que a organização mantenha dados reservados na nuvem privada, e disponibilize os demais na nuvem pública.

Até o momento, o trabalho apresentou diversas relações de ações computacionais que integram o ciclo de vida de um dado e as características que que se conjugam com a Segurança da Informação e que servem de arcabouço teórico para associar os padrões da área da saúde escolhidos, o Padrão TISS e o HL7.

Aprovado pelo *American National Standards Institute*[41] (ANSI), o padrão HL7 se refere ao modelo com mais alto nível de comunicação da *International Standards Organization*[42] (ISO) para sistemas abertos.

Na Portaria nº 2.073, de 31 de agosto de 2011, Capítulo II, o Ministério da Saúde estabeleceu o padrão HL7 para a interoperabilidade de sistemas que estejam compartilhando, em especifico, os resultados e solicitações de exames (BRASIL, 2011).

De acordo com a *International Association for Development of the Information Society*[43] (2004) o HL7:

> *supports such functions as security checks, participant identification, availability checks, exchange mechanism negotiations and, ost importantly, data exchange structuring. In September 2000, the HL7 membership ratified Version 1 of the Clinical Document Architecture (CDA), which defines an XML architecture for exchange of clinical documents. The encoding is based on XML DTDs (Document Type Definition) included in the specification and its semantics are defined using the HL7 RIM (Reference Information Model) and HL7 registered coded vocabularies.*[44]

Importante ressaltar que o modelo HL7 realiza a troca de arquivos em XML, ou seja, troca de informações por meio de uma rede sem fio, realizada por um *webservice*[45], o que torna essa troca de dados exposta e, consequentemente, mais vulnerável.

Quanto à segurança, esse modelo exige uma garantia de segurança específica do *hardware*, como os *firewalls* (ANSI, 2004, p.482), sendo necessário também respeitar a instalação correta de sistemas operacionais compatíveis. A ANSI (2004) afirma ainda que a segurança do *software* seja fornecida para o sistema através de sua arquitetura, confirma que "*any public network connection is a potential security weakness*"[46].

---

[41] Tradução livre: Instituto Nacional Americano de Padrões
[42] Tradução livre: Padrões de Organização Internacional
[43] Tradução livre: Associação Internacional para o Desenvolvimento da Sociedade da Informação
[44] Tradução livre: "suporta funções como verificações de segurança, identificação do participante, verificações de disponibilidade, troca negociações de mecanismo e, mais importante, estruturação de troca de dados. Em setembro de 2000, foi ratificada a Versão 1 da Arquitetura de Documento Clínico (CDA) do HL7, que define um XML arquitetura para troca de documentos clínicos. A codificação é baseada em XML DTDs (Tipo de Documento Definição) incluída na especificação e sua semântica são definidas usando o HL7 RIM (Referência Modelo de Informação) e vocabulários codificados registrados no HL7."
[45] Tradução livre: serviço de internet.
[46] Tradução livre: Qualquer conexão de rede pública é um ponto fraco de segurança potencial.

A saber, o modelo HL7 CDA (Clinical Document Architecture), já apontado no item 1.3 do Capítulo 1, junto aos demais padrões da saúde, impõe restrições mínimas na estrutura do documento e no conteúdo para a troca, de modo que as barreiras estruturais tornam a aplicação mais segura na troca de dados clínicos (ANSI, 2004, p. 483).

O *Intoperability of Eletronic Health Records*[47] (iEHR) apresenta informações básicas sobre os padrões de interoperabilidade em saúde, como o HL7 CDA[48] e o HL7 FHIR[49]. A arquitetura padrão do sistema HL7 CDA está desenvolvida em 3 (três) níveis, conforme representa a Figura 08.

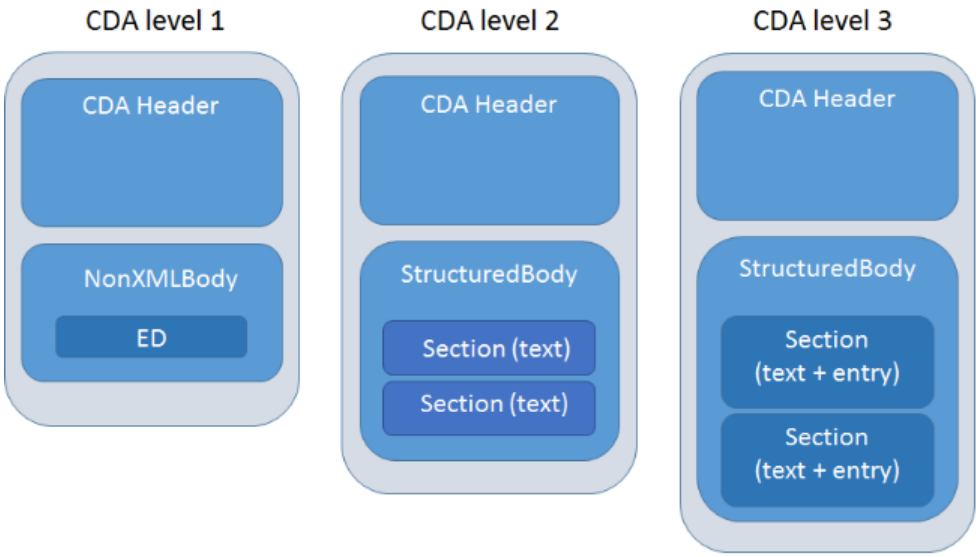

Figura 08: Níveis do CDA. Fonte: *Interoperability of eletronic health records* (http://iehr.eu/knowledge/what-is-hl7-cda/)

O nível 1, representa o detalhamento de notas clínicas narrativas padrões, como as especificações em cabeçalho. Já o nível 2, começa a dar "corpo" ao documento clínico do paciente pois admite em algumas de suas sessões que o profissional preencha em campos obrigatórios as informações a respeito dos "sinais vitais" , "histórico e físico", "exame físico", e uma seção opcional de "exame cardiovascular", "avaliação" e "plano" de tratamento (iEHR[50]).

---

[47] Tradução livre: Interoperabilidade de Registros Eletrônicos de Saúde
[48] Clinical Document Architecture (CDA)
[49] Fast Healthcare Interoperability Resources (FHIR)
[50] http://iehr.eu/about-us/

Por fim, o nível 3 do CDA corresponde à permissão de extração em um determinado nível de um documento clínico em que é permitido realizar uma descrição detalhada dos sintomas do paciente e descobertas do estado clínico, além de possibilitar uma gestão do faturamento através do preenchimento de códigos/autorizações de acesso (iEHR[51]).

Dessa forma, a possibilidade de preenchimento de dados em diferentes níveis exige uma aplicação de *software* compatível que, por sua vez, implementará a segurança necessária ao sistema, ampliando o leque de segurança das informações clínicas do paciente.

Em contrapartida, as características que compõe a edificação do Padrão de Troca de Informação da Saúde Suplementar (TISS) registra uma identificação quanto a troca eletrônica de informações em arquivos XML e, no entanto, prevê meios de garantia de integridade das informações como algoritmos de *hash* na função MD5 e certificados digitais/assinaturas digitais para autenticação, comunicação segura e integridade de dados (ANS,2012).

O *hash* MD5, tecnicamente chamado de Algoritmo MD5 *Message-Digest,* é uma função *hash* criptográfica cujo objetivo principal é verificar se um arquivo se mantém integro e sem alterações. Para isso, o MD5 compara (por meio de procedimento de soma) conjuntos de dados para verificar se são iguais, resultando na conclusão positiva ou negativa sobre a integridade do arquivo original.

Segundo De Holanda e Fernandes (2011, p.10) um dos principais fatores causadores de vulnerabilidades é a codificação ingênua do software por um programador, quando o mesmo considera basicamente os cenários positivos de execução de um código, sem se preocupar com o caso de usuários maliciosos e possíveis falhas.

Nessa circunstância, De Holanda e Fernandes (2011, p.24) exploram a possibilidade de criar vulnerabilidades para reparar antecipadamente essas falhas, e afirmam que essas vulnerabilidades são geralmente relacionadas com a indisponibilidade, a divulgação indevida de informação e a perda de integridade da informação.

---

[51] http://iehr.eu/about-us/

Logo, *softwares* que checam a integridade de arquivos de um sistema operacional usando a *hash* MD5 poderiam ser burlados utilizando-se da injeção de vetores (MIKLE, 2004), apresentando riscos onde a assinatura digital está presente.

Aplicando essa narrativa aos prontuários médicos, aqueles escritos em código orientado pela *web,* assim como demais sistemas que utilizam essa categoria, a exemplo do TISS estruturado em XML, com a utilização da função *hash* MD5 para assinatura, podem sofrer alterações desautorizadas através da injeção de vetores que geram o diagnóstico do paciente, causando colisão de informações que comprometem a integridade da assistência a saúde.

Portanto, considerando a vulnerabilidade que o *hash* MD5 se apresenta, pode-se dizer que essa função não seria a ideal para garantir a integridade de um dado na sua entrega à outro sistema, colocando em risco também autenticidade da informação.

De todo modo, ainda que os padrões insiram ferramentas de segurança para manter a integridade e confidencialidade do dado nas transações entre demais sistemas, não se pode falar na mitigação de riscos em sua totalidade.

Mesmo porque, quando se trata de ferramentas tecnológicas, as mudanças e atualizações em constante movimento, podem se sobrepor ao bom funcionamento de sistemas em detrimento de outros interesses e, além de tudo, o dever legal de cumprimento da legislação pátria em vigor adiciona pesos e contrapesos às ações de armazenamento e gerenciamento de dados empresariais, o que vem inflexibilizar a ocorrência de incidentes de segurança.

2.4. O ciclo de vida dos dados e os limites aos direitos fundamentais

O uso da tecnologia como ferramenta de informação e comunicação (TIC) para melhor entrega de serviços de saúde, muitas vezes, coloca em risco a intimidade e a privacidade dos titulares de dados ao fornecer informações pessoais compartilhadas na base de dados de sistemas interoperáveis. Isso porque, como visto no item 2.3 desse capítulo, a segurança de um *software* para a transferência, ou seja, para o compartilhamento somado ao armazenamento e coleta de dados em uma rede, exige rigorosas interfaces de proteção, podendo comprometer a integridade da informação e a privacidade do paciente.

Comprovadamente já demonstrado, o acesso facilitado à rede mundial de computadores congrega inquestionáveis benefícios a vida social que, além da área

de saúde, incluem o acesso à educação, a informação, a comunicação, ao comércio eletrônico, etc., propiciando um ambiente democrático para que as pessoas compartilhem possibilidades e exerçam a liberdade de expressão.

Mikhail Cancelier (2017, p.228) traz um elemento de alerta, afirmando cautelosamente que esse movimento massificado de acessos à internet, dificultou a imposição de barreiras à privacidade:

> O que se percebe é que com a popularização da internet, para além da intensificação da invasão da privacidade, a população passou a exercer um movimento de evasão da privacidade, enaltecendo a exposição deliberada de suas informações privadas.

Com a recente entrada em vigor da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (LGPD), em vigência desde setembro de 2020, o tratamento aos dados pessoais ganharam uma nova roupagem e proteção, uma vez que tratam da vida privada do indivíduo e devem obedecer aos requisitos legalmente determinados para a sua coleta, atento à manifestação de vontade do titular e de preservação da sua intimidade, (re)afirmando limites (BRASIL, 2018).

O escopo da LGPD é o tratamento de dados pessoais, em meio físico ou digital, por pessoa natural ou por pessoa jurídica, de direito público ou privado. A Lei também objetiva a proteção aos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, devendo ser observada pela União, Estados, Distrito Federal e Municípios, incluindo a Administração direta e indireta, inclusive fundações, empresas públicas e sociedades de economia mista (BRASIL, 2018).

A Lei que define para tratamento de dados ao exemplificar ao menos 20 (vinte) ações (art.5º, LGPD) (BRASIL, 2018), orienta um “ciclo de vida” dos dados: modo sequencial de ações que resultam em decisões na utilização/manutenção do dado.

Ricardo C. Sant´anna (2016, p.119) inicia a análise do ciclo de vida de dados ponderando a necessidade específica para qual se pretende coletar determinado dado, com o enfoque voltado a viabilidade e a um plano de ação definido. Inclusive, nesse primeiro momento, são feitos questionamentos para alinhar ao resultado pretendido, podendo exemplificar alguns em destaque: qual o escopo da necessidade informacional? Quais dados serão necessários? Como esses dados podem ser coletados e qual sua fonte? A coleta desses dados proporcional algum tipo de risco a privacidade para os indivíduos ou para as entidades referenciadas por eles?

Em seguida à obtenção desses dados pessoais, passa-se a fase em que os esforços são voltados ao armazenamento desse conteúdo, que exige o planejamento e a execução de ações que priorizam o conhecimento mais profundo da Ciência da Computação e Ciência de Dados (*Data Science*) para validar os modelos de estruturas definidos para os dados.

Após, inicia-se a fase de recuperação, em que os esforços são voltados para que os dados possam ser encontrados, acessados e interpretados. Em determinadas situações há chances de se verificar que os dados coletados já não são necessários e devem ser excluídos da base, o que leva a última fase: o descarte.

Para essa fase final também são exigidos conhecimentos específicos para a execução, uma vez que além da atividade técnica, a ação requer o aval e acompanhamento dos usuários envolvidos.

Diversos autores e instituições propuseram ciclo de vida de dados abordando processos que se assemelham em várias etapas. Santana (2013) destaca que não é possível abordar o processo de ciclo de vida sem considerar o contexto em que os dados devam ser tratados, bem como sua especificidade, seja administrativa, descritiva, técnica estrutural ou de preservação.

Inclusive, Briney (2015) entende pela existência de considerar uma nova perspectiva em face do ciclo de dado, uma vez que o valor dessa representação constitui uma parcial sistemática do assunto representado. Portanto, a autora inclui processos considerados relevantes, a exemplo do “compartilhamento de dados”, “preservação” e o “reuso” como processos de pesquisa, além de incluir “planejamento e gerenciamento de dado e projeto”, “divulgação de dados”, dentre outros representados pela Figura 09.

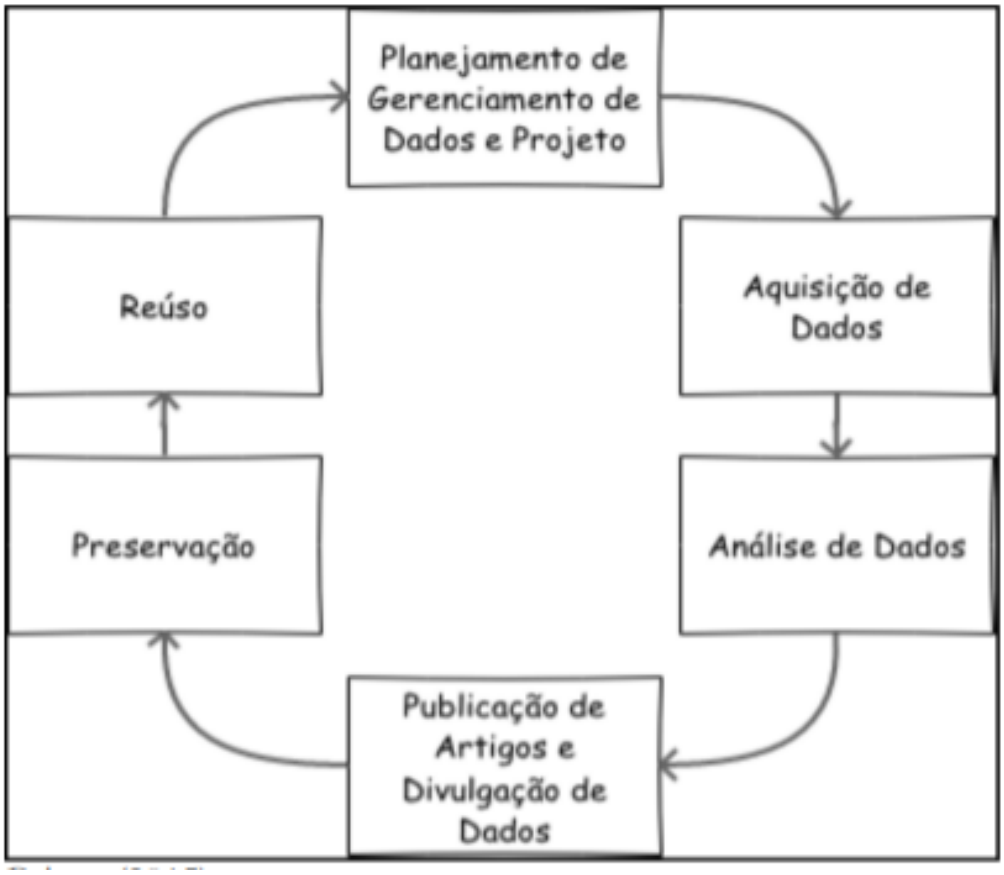

Figura 09: Ciclo de vida de dado (novo). Fonte: Adaptado de (BRINEY, 2015)

Sant´anna (2016, p.123) ainda salienta que além dessas fases, há fatores que estão presentes em todas elas, que são: privacidade, integração, qualidade, direitos autorais, disseminação e preservação.

Como resultado do ciclo de vida dos dados, o compartilhamento está dentre as prováveis ações no curso da utilização do conteúdo, além disso, no processo de gerenciamento da base é exigido pela LGPD o planejamento estratégico para garantir a segurança das informações (BRASIL, 2018).

Isto porque, os riscos de violação a dados pessoais, resulta em afronta aos princípios da dignidade da pessoa humana, quando por falta de barreiras de segurança capazes de reduzir vulnerabilidades.

Ocorre que, os instrumentos de tecnologia, atualmente, são considerados “pontes” de acesso à informação e, por consequência, uma condição para a garantia dos direitos individuais dessa liberdade, do direito da informação (SALDANHA; BRUM; MELLO, 2016).

Como o viés deste trabalho é voltado a segurança de dados pessoais sensíveis compartilhados em sistemas interoperáveis de saúde privado, sem sombra

de dúvida, na aplicação do ciclo de vida do dado o compartilhamento é meio de utilização para alimentar a base do PEP e RES do paciente assistido.

Neste ponto, não restrito apenas a entidades privadas mas também trazendo à baila o dever adstrito ao Poder Público que por intermédio da Lei de Acesso à Informação (LAI) nº 12.527 de 2011, objetiva o dever de informar e ser transparente quanto aos seus atos, prestando contas sobre suas decisões à população (BRASIL, 2011).

Ainda que a LAI tenha trazido significativo avanço democrático no fomento ao acesso à informação e a transparência da Administração Pública, Carvalho (2014) indica uma problemática tensão perante a utilização de dados, sejam eles considerados públicos ou privados.

Isso porque, mesmo com a autorizada utilização desses dados, essa informação não deixa de ser privada do titular. Desse modo, torna-se frágil a relação esses dois polos, uma vez que a própria LAI, na redação dos arts. 3º e 4º, enfatiza a prevalência ao direito à informação, sobre o da intimidade. (BRASIL, 2011).

Importante ressaltar que, tanto na Constituição quanto na legislação infraconstitucional, o direito à privacidade é considerado direito fundamental e direito da personalidade, sendo tratado como uma figura jurídica que supera a dicotomia entre as esferas público e privado. O constituinte optou pelo uso dos termos “intimidade e vida privada”[52] (BRASIL, 1988) para fazer referência à privacidade, sendo essa última expressão também a opção do legislador ao elaborar o Código Civil de 2002 (CANCELIER, 2017).

Independentemente da forma como é designada nos diplomas, quando a privacidade é tutelada o cuidado se volta em contemplar “atributos da personalidade humana merecedores da proteção jurídica”, ou seja, o que “muda é tão somente o plano em que a personalidade humana se manifesta” (SCHREIBER, 2013, p. 13).

Sendo a privacidade componente essencial à formação da pessoa, indispensável à construção do indivíduo e de suas fronteiras com os demais, sua tutela vai ao encontro da promoção e proteção da dignidade da pessoa humana, fundamento norteador do nosso ordenamento jurídico (DONEDA, 2019).

---

[52] Art. 5º, X, CF: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

À vista do tratamento aos dados de saúde, a LGPD evidencia tutela especial (ver item 1.2 do Capítulo 1) que pretende resguardar, ainda mais, o titular/paciente da exposição, e reforçar a responsabilidade médica no sigilo ao exercício profissional.

E nessa perspectiva é possível visualizar, retomando aos documentos enunciados até o presente momento, duas situações em confronto: de um lado a ANS, conduzindo interesses públicos e privados (por parte dos profissionais e agentes de saúde, planos de saúde privado e cooperativas médicas) ao editar resoluções normativas de padronização do atendimento ao paciente, além de integrar o uso de ferramentas tecnológicas para a gestão da comunicação entre sistemas; do outro lado, os diplomas legais que contornam o Estado Democrático e que confirmam os limites de atuação diante de direitos e deveres mínimos que compreendem as garantias individuais, além das legislações complementares em vigor que regulamentam a atividade de empresas públicas e privadas na coleta de dados, assim como, recomendam padrões de segurança para o bom uso dessas informações.

Em ambos os casos, a concessão dos dados confere grande responsabilidade por parte do ente público ou privado em criar processos de gestão para armazená-los de forma segura, o que nem sempre acontece.

Do mesmo modo acontece com o compartilhamento, que sugere não apenas um sistema, mas sim dois, com alto potencial de segurança para realizar a troca de dados sem violá-los durante o curso.

Ciente disso, Machado (2018, p.199) afirma que a LGPD “busca resgatar direitos valiosos à personalidade, como a privacidade informacional que, não obstante seja tutelada de forma genérica pela nossa Lei Maior, necessita de uma atenção especial por parte do legislador infraconstitucional”, especialmente para atender demandas que vão além da prestação jurisdicional.

Ou seja, mesmo que os diplomas legais reforcem a proteção aos direitos individuais em face do tratamento de dados, de nada servirá se não houver gestão de empresas públicas e privadas para resguardar essas garantias.

Embora Bioni (2019, p. 245) afirme haver “assimetria” entre os titulares de dados e o Poder Público, uma vez que o ente estatal sempre foi visto como detentor de posição de proeminência, devido ao fato do interesse público possuir superioridade hierárquica em relação ao interesse individual, pensar em mecanismos (inclusive legais) e alternativas para resgatar o valor da “vontade” do titular de dados mostra-se pertinente e urgente.

Assim, a validação do ciclo de vida dos dados, tanto para o ente público como ao ente privado devem seguir os critérios de adequação da LGPD respeitando os requisitos de segurança, mas, além disso, devem respeitar os princípios individuais que dizem respeito a privacidade, autonomia da vontade e intimidade do usuário, garantindo uma coleta autêntica.

CAPÍTULO III – UMA ANÁLISE AOS EFEITOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS Nº13.709 DE 2018 E SUA APLICAÇÃO NOS PADRÕES DE ASSISTÊNCIA À SAÚDE SUPLEMENTAR

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, os dados foram elevados à importância da preservação à privacidade relacionada aos dados pessoais e sensíveis de cada indivíduo.

Considerando os critérios objetivos de segurança, consentimento, finalidade, e os princípios já tratados no Capítulo 2, passa-se para a abordagem das possíveis consequências no compartilhamento, inclusive a violação à privacidade, quando não respeitados as medidas apontadas pela LGPD na proteção aos dados pessoais sensíveis, com enfoque no trânsito de dados entre os sistemas interoperáveis da saúde.

3.1. Os direitos da personalidade no compartilhamento de dados sensíveis pelos agentes de tratamento

Naquilo em que se propõe a Lei Geral de Proteção de Dados nº 13.709 de 2018 (LGPD) no tratamento de dados pessoais, com o objetivo de proteção aos direitos fundamentais da liberdade e privacidade e o livre desenvolvimento da personalidade natural (BRASIL, 2018), inclui também a atuação das figuras que manipulam esses dados: os agentes de tratamento.

Para o bom funcionamento de todo o ciclo de vida dos dados, a tarefa realizada pelos agentes de tratamento (coleta, armazenamento, tratamento, transferência, etc.) complementam àquelas ações programadas para os sistemas interoperáveis, como visto no Capítulo 2.

Assim, dentro do gênero “agentes de tratamento” disposto na LGPD (art. 5º, IX), encontram-se duas espécies principais: o “controlador” e o “operador” (BRASIL, 2018).

O controlador é definido pela LGPD como “pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais” (art. 5º, inciso VI). Sua principal atribuição é o poder de decisão, o ato de definir os elementos essenciais de tratamento, determinando, em suma, sobre a coleta de dados, finalidade de uso, tempo de armazenamento e eliminação (BRASIL, 2018).

Em razão dessas prerrogativas o controlador assume uma série de responsabilidades, como a de elaborar o relatório de impacto à proteção de dados pessoais (art.38), inclusive dados sensíveis, manter à disposição do titular informações sobre o tratamento de seus dados (art.9º), e comprovar que o consentimento do titular observou as exigências legais e reparar os danos, caso o tratamento não ocorra conforme previsto na LGPD (art.8º, § 2º) (BRASIL, 2018).

No setor público, o controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada por uma pessoa física e autoridade responsável para a adoção de medidas acerca do tratamento de tais dados (art.5º, VI) (BRASIL, 2018).

Dessa forma cabe ao controlador justificar quais os motivos pelos quais optou pelo tratamento e como serão as ações tomadas para atingir a finalidade proposta. Afinal, ele é o agente responsável por todo o ciclo dos dados, desde a coleta até a exclusão efetiva (BRASIL, 2018).

Por sua vez, a LGPD indica como operador aquele que atua como pessoa “natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (art.5º, VII), podendo ser considerado também agente público – em sentido amplo – que exerçam tal função, ou pessoas jurídicas diversas daquela representada pelo controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere (BRASIL, 2018).

Diferentemente das atividades praticadas pelo controlador, o operador não controla os dados pessoais destinados ao tratamento, assim como é impossibilitado de modificar as finalidades ou autorizar o uso do conjunto particular de dados sob um determinado tratamento (art.9º,§2º), seu dever é efetivamente realizar o tratamento dos dados de acordo com as denominações e finalidades estabelecidas pelo controlador (BRASIL, 2018).

Mesmo que o exercício da função do operador seja restrito a atuação do controlador e com aquilo que é decidido por ele, é comum que lhe seja concedido um certo grau de discricionariedade e liberdade sobre os procedimentos de tratamento de dados. Sendo assim, o operador ganha o direito de exercer um determinado controle sobre as ações de tratamento e tem a permissão de decidir a maneira que os dados são tratados (art.5º, VII; art.39).

Para que os agentes de tratamento de dados possam exercer suas funções e direitos dentro da legalidade, a LGPD estabelece ao operador as seguintes responsabilidades (art. 37):

1) Obtenção de consentimento: específico do titular, quando necessário;
2) Informações e prestação de contas e pela garantia de portabilidade dos dados;
3) Garantia de transparência no tratamento de dados baseado em legítimo interesse;
4) Manutenção do registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse;
5) Reparação de danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais;
6) Comunicação à autoridade nacional e ao titular a ocorrência de incidente e segurança que possa acarretar risco ou dano relevante aos titulares;

Dessa maneira a LGPD consegue entregar ao operador a liberdade de utilizar seus conhecimentos técnicos e *expertise* nas ações de tratamento para que ele tenha o poder de decisão, de acordo com as normas e em nome do controlador, nas operações que serão utilizadas no tratamento de dados pessoais para um determinado objetivo.

A atuação em conjunto dos agentes de tratamento, controlador e operador, pode ser utilizada como ferramenta para auferir responsabilidade aos direitos personalíssimos já confirmados constitucionalmente para cada titular de dado. Isto é, em caso de qualquer tipo de violação e descumprimento da norma legal que tenha, como consequência, dano ao titular de dados, comprovado mediante nexo de causalidade, é dever dos agentes de tratamento a responsabilidade civil de reparação (art.42) (BRASIL, 2018).

No contexto da proteção de dados pessoais vinculado à assistência à saúde, Guilherme M. Martins e Carlos C. Teles (2021, p. 186) afirmam que a “natureza na responsabilidade civil no âmbito da LGPD, é tema controvertido” e por isso, o instituto merece ser visitado cautelosamente em cada corrente defendida.

Para Danilo Doneda e Laura Mendes (2018, p.555), o legislador, ao considerar a finalidade da lei e os princípios por ela adotados, optou por um regime de responsabilidade civil objetiva na atividade de tratamento de dados, ou seja, o risco

à violação de direitos fundamentais e personalíssimos é inerente, de modo que independe da aferição de culpa dos agentes de tratamento.

Por outro lado, Gisela Sampaio da Cruz e Rose Melo V. Meireles (2019, p. 231), defendem que a LGPD, adotou a teoria da responsabilidade civil subjetiva, de modo a exigir a comprovação da conduta culposa dos agentes de tratamento na ocasião do dano. Desse modo, mencionam as autoras duas prováveis situações em que haveria prova da culpa dos agentes: i) o disposto no art.44 da LGPD, quando o legislador faz menção as medidas de segurança, de modo que a omissão na observância dessas medidas pode levar ao estado de culpabilidade do agente; ii) o disposto no art. 43, II da LGPD, quando provado que o tratamento de dados foi feito de acordo com a legislação sendo, portanto, uma excludente de ilicitude referente ao cumprimento das normas da LGPD.

A terceira corrente, capitaneada por Maria Celina Bondin de Moraes e João Quinelato de Queiroz (2019, p. 118), adota a teoria de responsabilidade civil ativa ou proativa, isto é “que garanta ao titular o conhecimento pleno das formas de tratamento, finalidade e destino de seus dados”. Ou seja, é dever dos agentes de tratamento atuarem preventivamente na tutela à prevenção de danos, de modo que, antecipando com rigor as medidas de segurança, a obrigação de reparação em caso de dano é medida excepcional a ser tomada.

Importante ressaltar que os dados pessoais, por constituírem conteúdo do direito à privacidade, devem seguir as medidas rigorosas e eficazes de proteção, em especial à dados pessoais sensíveis, núcleo da dignidade da pessoa humana (MORAES; QUEIROS, 2019).

Assim, essa teoria também possui conjunção com a previsão do art. 6º da LGPD que reconhece o principio da responsabilização e preservação de contas, impondo aos agentes de tratamento de dados pessoais a “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas” (BRASIL, 2018).

Após sucintas definições de diferentes teorias da responsabilidade civil aplicadas aos agentes de tratamento de dados pessoais, retoma-se à importância da segurança utilizada pelos sistemas interoperáveis dos planos de saúde suplementar. Isso porque, ao nomear os agentes tratamento que serão responsabilizados pelas atividades executadas *in loco* que compõem todos os processos de tratamento de

dados, estes também poderão ser responsabilizados caso haja comprovada violação do sistema por ausência de segurança adequada.

Martins e Teles (2021) defendem que as operadoras de saúde que ofertam, como fornecedores de serviços, elementos “facilitadores” de compartilhamento de dados, informações de pacientes em prontuários eletrônicos (PEP) e que buscam maior extensão ao atendimento médico e hospitalar, sem dúvidas, estariam calçados na teoria da responsabilidade civil objetiva sob a luz do art. 42 da LGPD.

Ainda, sustentem que o risco se encontra intrínseco à responsabilidade do empreendimento, destacando este ponto da seguinte forma:

> A teoria do risco do empreendimento como orientação para que responsabilidade civil do fornecedor se dê de forma objetiva. O risco proveniente da atividade do fornecedor é suscetível de previsão antecipada, necessário para a proteção do consumidor vulnerável, o que também se aplica aos chamados riscos do desenvolvimento, isto é, aqueles que não podem ser cientificamente conhecidos no momento do lançamento do produto no mercado, contudo vindo a ser descoberto após a introdução no mercado e, causando danos ao consumidor, será responsabilizado o fornecedor, conforme previsto na legislação consumerista (MARTINS; RAMADA; FRANCO, 2020).

Ademais, imperioso se faz destacar que o profissional médico, levando em consideração a obrigação de meio e a responsabilidade subjetiva em relação ao tratamento médico (art. 14, §4º do CDC), enquanto operador ou controlador responderá de forma objetiva em relação ao tratamento de dados do paciente (MARTINS; TELES, 2021).

No exemplo dado por Martins e Teles (2021, p.192) da qual o profissional médico faz uso da técnica da telemedicina estando vinculado a qualquer plano de saúde privado e realiza o tratamento de dados pessoais em favor deste, enquadrar-se-ia, portanto, na qualidade de operador de dados. De outro forma, quando o profissional faz uso da mesma técnica, porém atuando de forma autônoma, em consultório próprio, tomando decisões referentes aos dados pessoais seus pacientes, enquadrar-se-ia como controlador.

Ora, tendo em vista a responsabilidade solidária atribuída aos agentes (controlador e operador) no art. 42, §1º, I e II, da LGPD, estes deixarão de ser responsabilizados quando não houver violação à legislação de proteção de dados que lhes são atribuídos ou quando realizados não houver violação à legislação de proteção, ou, ainda, quando decorrer de culpa exclusiva do titular de dos dados ou de terceiros (art. 43) (BRASIL, 2018).

Resta destacar que o art. 52 da LGPD, elenca as sanções administrativas aplicáveis aos agentes de tratamento em razão das infrações cometidas podendo acarretar multa de até 2% (dois por cento) incidente sobre o valor do faturamento da empresa, chegando até a monta de R$50.000.000,00 (cinquenta milhões de reais), além de outras sanções (BRASIL, 2018).

Dessa forma, sob a análise dos direitos da personalidade inseridos no contexto do tratamento de dados pelos profissionais de saúde, os controladores e operadores nomeados para a execução da função, deverão observar as medidas de segurança mínima imposta na proteção a esses direitos. Contudo, além do risco voltado à violação de sistemas, especialmente sistemas interoperáveis que realizam troca de informações em rede, a violação à privacidade do titular também deve ser fato considerado, inclusive por estar prevista pelo legislador no art. 42 da LGPD.

Portanto, em conclusão sobre a análise da reparação ao titular de dados em eventual hipótese da ocorrência de dano, a coerência que mais se aproxima é a aplicação da teoria da responsabilidade civil objetiva, observados os critérios mínimos de segurança previsto em lei, haja vista a vinculação da responsabilidade civil do agente frente ao risco de sua atividade, remetendo aos ditames do art. 927, § único do Código Civil (BRASIL, 2002).

3.2. A atuação dos agentes no tratamento de dados pessoais sensíveis e as medidas adequadas para a mitigação de riscos

Até aqui diversos pontos que compõe o tema dessa pesquisa já foram minuciosamente conceituados e colocados no presente contexto. Portanto, neste momento, retoma-se a atuação dos agentes de tratamento destacado no item anterior desde Capítulo e acrescenta as medidas possíveis e alternativas para mitigação de risco em sistemas de troca de informação.

O item 1.2 do Capítulo 1, enfatizou o rol de dados pessoais sensíveis que formam uma categoria diferenciada para fins de tutela da Lei Geral de Proteção de Dados Pessoais (LGPD).

Gustavo Tepedino e Chiara de Teffé (2020, p. 22) afirmam que os dados sensíveis são considerados o “núcleo duro da privacidade” de modo que, conforme o tipo e natureza de informação que trazem, constituem-se dados cujo tratamento pode ensejar em discriminação ilícita ou abusiva ao titular.

Complementando o que já foi delineado também no Capítulo 2, os dados pessoais sensíveis coletados com a finalidade de saúde fazem parte de bancos de dados e circulam entre sistemas interoperáveis, inclusive no âmbito da assistência à saúde suplementar.

Portanto, além das rigorosas recomendações de segurança desses sistemas, em especial por conterem dados e informações com alto grau de sigilo, a manutenção da integridade é tanto responsabilidade dos agentes de tratamento como de terceiros que o alimentam e o utilizam.

Em razão disso, a LGPD determina a observância de regras específicas para o tratamento de dados pessoais sensíveis, conforme disposto nos incisos do artigo 11 da LGPD (BRASIL, 2018), quais sejam:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
> § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
> § 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
> § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos

> os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
> I - a portabilidade de dados quando solicitada pelo titular; ou
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Pois bem, no âmbito de aplicação da LGPD, o artigo 11, em seu parágrafo primeiro, vem expressamente reforçar o dever de aplicação dos incisos a qualquer tratamento de dados pessoais que se revele como “dados pessoais sensíveis” (BRASIL,2018). No entanto, parece clara a expressão desse artigo no que se refere a aplicação em todas as hipóteses em que os dados pessoais não possuam a característica de “sensível”, mas que possam “revelar”, de alguma maneira, dados sensíveis (BIONI, 2019).

Para Mulholland (2021, p. 10), a redação do artigo 11 é aplicável a qualquer tratamento de dados pessoais, de modo que estaria vinculada a hipótese de geração de dano ao titular qualquer forma de violação desses incisos. Ou seja, a aplicação do artigo 11 da LGPD, somente estaria legitimada se o tratamento de dados pessoais que revela dados sensíveis gerar algum dano ao titular dos dados.

Dessa forma, a correta interpretação do texto legal, direcionado ao entendimento seria de que o “tratamento de dados pessoais sensíveis gerará sempre danos de natureza personalíssima por violação aos direitos de privacidade, liberdade ou identidade, fundamentos da proteção de dados” (MULHOLLAND, 2021), isso porque, o risco é intrínseco à atividade.

Ainda, neste mesmo artigo, os parágrafos 3º e 4º estabelecem que a comunicação ou o uso compartilhado de dados sensíveis, com o objetivo de obtenção de vantagem econômica, poderá ser vedada ou regulamentada pela autoridade nacional competente (BRASIL, 2018).

No entanto, existem hipóteses em que é admitido o compartilhamento de dados pessoais sensíveis referente à saúde, sejam elas: assistência farmacêutica, assistência à saúde – incluídos os serviços auxiliares de diagnose e terapia – em benefício aos interesses dos titulares de dados, e para permitir a portabilidade de dados quando solicitada pelo titular; ou no caso de transações financeiras e

administrativas resultantes do uso e da prestação dos mencionados serviços[53] (art. 11, §4º, I e II) (BRASIL, 2018).

Dessa forma, resta evidente que a proteção aos dados pessoais sensíveis está intimamente ligada com a conduta adotada pelo agente de tratamento (controlador e operador), uma vez que o manuseio de informações sigilosas de cunho íntimo pode acarretar graves prejuízos ao titular. A vista disso, os artigos 42 a 45 da LGPD se referem à natureza da obrigação de indenizar o titular que sofre dano em razão da violação de sua intimidade no tratamento de seus dados (BRASIL, 2018).

Portanto, faz-se imprescindível relembrar o item anterior deste Capítulo, que traça duas probabilidades de imputar-se a responsabilidade ao agente: a) subjetiva – baseada na conduta culposa do agente de tratamento – ou b) objetiva – fundamentada no risco da atividade desenvolvida pelos agentes, controlador e/ou operador (MULHOLLAND, 2021).

Para de Mulholland (2021, p.11), a imputação da responsabilidade está sujeita as condutas dos agentes que poderão ser justificadas pela ação de 03 (três) princípios essenciais elencados na LGPD (art.6º), quais sejam: (i) segurança[54], (ii) prevenção[55] e (iii) responsabilização e prestação de contas[56], além de complementarem aos artigos 46 e seguintes da LGPD[57] que tratam da segurança de dados, governança e sanções administrativas adequadas na ocorrência de incidentes de segurança.

Assim, ao fazer uma relação da responsabilidade civil dos agentes de tratamento com a coleta de dados dos pacientes submetidos às clínicas médicas e hospitalares que cedem dados para complementar a base de padrões da saúde voltados à assistência suplementar – o cerne dessa pesquisa – torna-se possível

---

[53] O art. 11, § 5º, da LGPD, ainda ressalta que as operadoras de planos privados de assistência à saúde não podem tratar dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

[54] Art. 6, VII, LGPD - segurança: utilização de medidas técnicas e administrativas aptas a proteger os da 8 - dos pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

[55] Art. 6, VIII, LGPD - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do 9 tratamento de dados pessoais

[56] Art. 6, X, LGPD - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de 10 medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[57] Art. 46, LGPD. 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 de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

identificar pontos relevantes para a conduta tanto dos profissionais quanto de terceiros no tratamento dessas informações.

Por isso, é preciso atenção aos *standards* quando da conduta dos agentes de tratamento de dados, especialmente os padrões voltados à segurança da informação, sigilo, boas práticas e governança.

3.3. A implementação do Programa de Governança em Privacidade como ferramenta para a proteção de dados

Com a crescente demanda, o tratamento de dados pessoais passou a agregar grandes empresas e grandes economias, requerendo cada vez mais uma prestação jurisdicional por parte de legislações específicas para tutelar a atividade, assim como a Lei Geral de Proteção de Dados Pessoais (LGPD), além da criação de mecanismos de adesão por parte das empresas à normas éticas e legais de conformidade. Um dos *standards* recomendados para a qualidade técnica e cumprimento do dever legal é a governança corporativa.

A governança corporativa é exemplo de norma a ser incorporada por empresas e organizações que atuem nos mais variados ramos, aqui em especial na saúde, uma vez que, apesar do conceito econômico e político bastante abrangente, e da atuação de diversos agentes, é um sistema pelo qual as companhias são dirigidas e controladas (CADBURY COMMITTEE, 2019). Assim, a atividade busca primordialmente incentivar e manter as condições de boas práticas, possibilitando que a empresa cumpra com o seu papel social e atinja os resultados esperados (ALMEIDA, 2019).

Para a OCDE (Organização para a Cooperação e Desenvolvimento Econômico), a governança é tida como guardiã de direitos:

> A governança coorporativa é o sistema segundo o qual as corporações de negócio são dirigidas e controladas. A estrutura da governança corporativa especifica a distribuição dos direitos e responsabilidade entre os diferentes participantes da corporação, tais como o conselho de administração, os diretores executivos, os acionistas e outros interessados, além de definir as regras e procedimentos para a tomada de decisão em relação às questões corporativas. E oferece também bases através das quais os objetivos da empresa são estabelecidos, definindo os meios para se alcançarem tais objetivos e os instrumentos para se acompanhar o desempenho.

Os agentes de tratamento de dados pessoais – controlador e operador –, no âmbito de suas competências, com relação ao tratamento de dados, podem elaborar

individualmente ou por intermédio de associações regras de boas práticas e de governança, que determinam as condições de organização, os padrões técnicos a serem utilizados, as normas de segurança, dentre outros (art. 50 da LGPD) (BRASIL, 2018).

Ao estabelecer as referidas regras, os agentes devem levar em conta, no que se refere ao tratamento e aos dados: a natureza, o escopo, a finalidade e a probabilidade, bem como, a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular (art.50, §1º) (BRASIL, 2018).

Devido à complexidade de determinados setores e atividades de tratamento, a ferramenta de gestão e de boas práticas servem de aliadas dos agentes de fiscalização e *enforcement*[58], pois atuam como instrumento para mitigação de riscos e aproximam-se do melhor cumprimento da legislação com os agentes de tratamento.

Essas ferramentas não devem estar restritas ao setor privado, mas também devem ser aplicadas ao setor público, conforme disposto no artigo 32 da LGPD, que prevê que a autonomia da Agência Nacional de Proteção de Dados (ANPD) para sugerir a adoção de padrões e de boas práticas para o tratamento de dados pessoais, quando esse tratamento for realizado pelo Poder Público (BRASIL, 2018).

Importante relembrar que a ANPD é a responsável por zelar pela proteção dos dados pessoais, com base na legislação; por elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; por fiscalizar e aplicar as sanções nos casos de tratamento de dados que descumprirem a legislação, por meio de processo administrativo, que assegure o contraditório, a ampla defesa e o recurso, entre outros (art. 55-J, IV) (BRASIL, 2018).

Portanto, para o bom funcionamento, as regras de boas práticas e de governança devem ser atualizadas e publicadas de maneira periódica e podem ser reconhecidas e divulgadas pela ANPD (art.50, §3º) (BRASIL, 2018).

Outro *standard* de importância previsto pela LGPD, fazendo agora referência ao inciso I do artigo 50, é a implementação do Programa de Governança em Privacidade – PGP (BRASIL, 2018).

O PGP pode ser entendido como o conjunto de regras de boas práticas e de governança que determinem as condições de organização, o regime de

---

[58] Tradução livre: aplicação

funcionamento, os procedimentos, as reclamações dos titulares, as normas de segurança, os padrões técnicos, as obrigações para os envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de diminuição de riscos e outros aspectos referentes ao tratamento de dados pessoais (BLUM; MORAES, 2020).

Salienta-se que o PGP deve levar em consideração a estrutura de governança corporativa existente na organização frente ao risco da atividade enfrentada pelos agentes de tratamento. Segundo o Instituto Brasileiro de Governança Corporativa (IBGC, 2015), o PGP equipara-se à governança corporativa que pode ser entendida como um sistema por intermédio do qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre os sócios, os conselhos de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

Adiante da redação do artigo 50 da LGPD, no parágrafo 2º, são indicadas as características mínimas que deve conter um Programa de Governança em Privacidade – PGP, sejam elas (BRASIL, 2018):

1) O comprometimento do controlador na adoção de processos e políticas internas que assegurem o cumprimento, de maneira abrangente, de normas e boas práticas relacionadas à proteção de dados pessoais;

2) A aplicação a todo o conjunto de dados pessoais que estejam sob o seu controle, independentemente da forma como foi realizada a coleta;

3) A adaptação à estrutura, à escala e ao volume de suas operações, assim como, à sensibilidade dos dados tratados;

4) O estabelecimento de políticas e salvaguardas de acordo com o processo de avaliação sistemática de impactos e riscos á privacidade;

5) O estabelecimento da relação de confiança com o titular, por intermédio da atuação transparente e que assegure mecanismos de participação do titular;

6) A integração da estrutura geral da governança, o estabelecimento e a aplicação de mecanismos de supervisão internos e externos;

7) Com planos de resposta a incidentes e remediação;

8) A atuação constante com base nas informações obtidas a partir do monitoramento contínuo e avaliações periódicas.

É prudente os planos de saúde suplementar, assim como as demais empresas médicas e hospitalares que exploram o serviço à saúde, desenvolvam seus programas de governança em privacidade, unindo as características acima elencadas, com a previsão de processos e políticas internas que assegurem o cumprimento de normas e boas práticas de segurança relativa a proteção de dados pessoais sensíveis.

Transpondo a utilização dos sistemas interoperáveis e a exposição de direitos fundamentais dos titulares de dados armazenados e compartilhados, verifica-se que o item 4 reitera a sistemática de salvaguarda dos dados pessoais, voltados com a preocupação de riscos à privacidade mas que, aliado ao item 7, pode mitigar a ocorrência de danos neste sentido.

Ainda, o Guia de Elaboração do Programa de Governança em Privacidade (2020) delimita a estruturação do PGP que deve obedecer às seguintes etapas:

1) Iniciação e planejamento: compreende quais são as primeiras informações e os dados importantes que devem ser conhecidos; a nomeação do encarregado; o alinhamento de expectativas com a alta administração; o diagnóstico do atual estágio de adequação à LGPD; a análise e adoção de medias de segurança; incluindo as diretrizes e a cultura interna; a instituição de estrutura organizacional para governança e gestão da proteção de dados pessoais; o inventário de dados pessoais e o levantamento dos contratos referentes a dados pessoais (GOVERNO FEDERAL, 2020).

Nessa etapa também deve ser criada uma estrutura organizacional para compor o conhecimento de dados pessoais na entidade ou órgão, para supervisionar as três etapas da ação para criar e manter o Programa de Governança em Privacidade.

2) Construção e Execução: aqui leva-se em consideração o gerenciamento de direitos individuais; o consentimento e o rastreamento de preferências e a redução de responsabilidade por violação.

Os marcos para serem alcançados nessa fase são: as políticas e práticas para a proteção da privacidade do cidadão; a cultura de segurança e proteção de dados e *Privacy by Design*; o Relatório de Impacto à Proteção de Dados Pessoais – RIPD; a Política de Privacidade e Política de Segurança da Informação; a Adequação de cláusulas contratuais e os Termos de Uso (GOVERNO FEDERAL, 2020).

3) Monitoramento: essa etapa inclui os indicadores de performance, a gestão de incidentes, a análise e o reporte de resultados. Entre os indicadores de

performance cabe apontar: os índices de serviço com dados pessoais inventariados, os índices de serviços com termos de uso elaborado, o índice de conscientização em segurança, entre outros.

A reunião dessas três etapas dentro de uma estrutura organizacional de suporte a saúde propicia fluidez no serviço prestado pelos agentes de tratamento e profissionais médicos, além de elevar as chances de bons resultados práticos, evitando a ocorrência de exposições dos titulares e infrações à privacidade.

Ou seja, na sequência dessas etapas, projetando a coleta de dados para a saúde, dar-se-ia da seguinte maneira: 1) inicia-se com a criação de uma estrutura organizacional e administrativa que se propõe a escolher uma equipe especializada, nomear agentes de tratamento, definir de quais dados dos pacientes serão necessário na coleta para o resultado pretendido (ex: nome, CPF, CEP, endereço, filiação, idade, etc.), buscar a legislação que trata sobre saúde e elaborar documentação necessária (ex: Termos de Consentimento Livre e Esclarecido) para o consentimento do paciente, aderir a processos informatizados que facilitem a reunião dessas informações (seja próprio ou terceirizado) e traçar planos de contingência para mitigação de erros, tanto operacionais como de equipes ; 2) entender as necessidades de funcionamento do negócio e incorporar políticas para melhor estruturação das práticas, ou seja, normas internas e externas a serem seguidas para o melhoramento da atividade e redução dos impactos negativos; 3) por fim, cabe o monitoramento das atividades dentro da estrutura criada e acompanhamento dos resultados.

Nessa mesma perspectiva criar etapas para um bom processo de gestão, pensando na Segurança da Informação, a norma ISO/IEC 27001:2006 visa estabelecer, implementar, operar, monitorar e analisar criticamente a decisão estratégica de uma organização. Visa ainda a melhoria contínua da segurança da informação que representam as várias atividades diárias que são necessárias para um programa de segurança eficaz e ativo (ABNT, 2006).

Ou seja, muito além do Guia de Elaboração de Programa de Governança em Privacidade (2020), o Programa de Governança em Privacidade (PGP) propõe um “caminho ideal” que deve ser percorrido por uma estrutura organizacional para atingir determinado resultado. Assim, quando a preocupação é o tratamento de dados pessoais sensíveis, não basta somente conferir esse percurso, mas sim identificar as

falhas que podem colocar a privacidade e intimidade do titular em risco, e, por fim, buscar afastá-las ou evitar que elas ocorram.

Para melhor entendimento, Maurício R. Lyra (2015, p. 59) diferencia “gestão” e “governança”, afirmando que a governança da segurança da informação tem a missão de descentralizar a gestão da segurança da informação de forma eficiente e transparente, aliado ao resultado fim entregue pela organização, levando em consideração os objetivos estratégicos e tendências atuais do mercado.

Para melhor entendimento: se, hipoteticamente, um estabelecimento médico, que possua acesso a prontuários eletrônicos de paciente, exames, resultados de exames, laudos, prescrições, e etc., cria seu Guia de Elaboração de Programa de Governança em Privacidade indicando em um de seus itens que opera com “segurança nos procedimentos de armazenamento e compartilhamento em nuvem”. Entretanto, para entender como essa segurança funciona, ou como ela pode ser acionada (para fins de melhoria ou substituição), a estrutura de governança da segurança é quem irá indicar as possibilidades e mecanismos para “testar” esses procedimentos, seja através de tentativas de invasão ou respondendo a ataques de vulnerabilidades.

Como já visto no Capítulo 1, item 1.4, o sistema de gestão aplicado para se atingir resultados é o PDCA que propicia melhoria continua de processos e produtos dentro de uma organização. O SGSI, também já visto, como um sistema de gestão que é criado pela ISO/IEC 27000, faz uso do PDCA para a delimitação de uma estratégia bem definida, objetivos de criação, manutenção, melhoria, revisão, funcionamento e análise de processos.

Dentro das métricas de gestão, chama atenção para o contexto da proteção de dados no âmbito da saúde uma estruturação coorporativa consciente nos riscos e consequências da sua atuação (LYRA, 2015). Partindo dessa realidade, é possível incorporar treinamentos para equipes técnicas que atuem na manipulação e gerenciamento de dados de titulares/pacientes/beneficiários, como também aderir a programas de gestão de segurança para a contenção de vulnerabilidades ou com rápida resposta à incidentes.

Evidentemente que na atuação de planos de saúde privado, este como uma organização corporativista própria, possui sua estrutura organizacional que deve ser respeitada pelos profissionais médicos que a utilizam como intermediadora do acesso à saúde. Portanto, muito além do profissional, os demais encarregados também

seguem diretrizes de conduta para que todo o procedimento administrativo, desde a recepção do paciente até o armazenamento de dados após a finalização da consulta/procedimento com o paciente, seja fluído e seguro.

Ainda, como resultado da implementação da LGPD e com base nessa estrutura e métodos para a mitigação de riscos, a ANS publicou a Resolução Normativa nº 443 de 25 de janeiro de 2019, que dispõe sobre a adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos para o setor da saúde (ANS, 2019).

Com essa normativa, a ANS estimula a redução do risco de descontinuidade de operações de planos de saúde decorrentes de falhas de controles internos e baixa capacidade de gestão ameaças das quais as operadoras estão expostas, o que pode comprometer em grande proporção a assistência prestada aos beneficiários (ANS, 2019).

A normativa estabelece que as práticas e estruturas adotadas pelas operadoras devem considerar os princípios de transparência, equidade, prestação de contas e responsabilidade corporativa, sendo atribuição dos administradores das operadoras a implantação, implementação e avaliação periódica das práticas de governança, gestão de riscos e controles internos que trata a normativa (ANS, 2019).

Ainda, impõe a obrigatoriedade às operadoras de grande e médio porte (exceto aquelas classificadas na modalidade de autogestão por RH), a partir de 2023 o envio anual do “Relatório de Procedimentos Previamente Acordados – PPA”, elaborado por auditor independente, tendo por base os dados do exercício anterior referentes aos processos de governança, gestão de riscos e controles internos (ANS, 2019).

Portanto, a incorporação de medidas e recomendações legais a serem gradualmente adotadas pelas organizações, além de cumprir com a expressão da Lei, podem também representar destaque perante o mercado, passando confiança ao cliente/usuário do serviço/titular de dados que o alimenta.

3.4. Uma perspectiva sob as ferramentas de gestão adotadas pelo padrão informatizado na saúde suplementar (TISS)

A padronização acompanha o desenvolvimento da História da Humanidade, mesmo que imperceptível aos olhares da sociedade. Pois, para que um processo de

comunicação se torne efetivo, é necessário que os envolvidos compreendam a linguagem envolvida nesse processo.

No contexto das organizações, tal entendimento também se faz necessário e, naquelas cujo ramo da atividade é a saúde, isso se torna ainda mais urgente para que os ruídos – que naturalmente surgem entre os serem humanos – sejam reduzidos e a comunicação se torne mais compreensível entre os envolvidos. Segundo Jannuzzi (1999, p. 24):

> (...) a grande diversidade de aplicações de conceitos e termos tem resultado em um significativo ruído comunicacional, interferindo na fluidez necessária ao processo. Mas, eliminar ruídos implica, antes de tudo, que os envolvidos estejam falando “a mesma língua”, ou seja, basicamente um padrão.

A padronização é elemento facilitador da atividade médica e hospitalar, pois os dados armazenados nos sistemas de informação são importantíssimos para o cuidado do paciente e para a gestão de instituições. Caso contrário, com o volume de termos e conceitos (terminologia), os profissionais e especialistas da área não conseguiriam comunicar-se de maneira linear, tampouco repassar as informações gerenciais e de saúde dos pacientes de forma organizada e fiel (DIAS, 2000).

Mesmo com a adoção da padronização por diversas especialidades de atuação médica, além da interoperabilidade de sistemas que atuam em conjunto, há eventos de fragmentação de informações em sistemas independentes, o que conduz a um parcial acesso aos elementos necessários de identificação para a tomada de decisões. Tal fato apresenta riscos aos pacientes já que as condutas dos profissionais de saúde são tomadas a partir de informações que constam em seus prontuários eletrônicos e que, no caso da fragmentação, apresentam-se incompletas.

As questões de padronização e interoperabilidade não pertencem somente a computação e sistemas informatizados, devendo ser tratada pelos profissionais de saúde, por gestores da área de saúde e por profissionais da Ciência da Informação como peça fundamental para a qualidade da assistência e do cuidado aos pacientes.

Repetições de exames, rupturas na continuidade do cuidado com o paciente e ruídos nas informações utilizadas nas tomadas de decisão relacionadas às políticas públicas de saúde resultam alto custo para as organizações e prolongamento no atendimento ao paciente.

Como meio de redução desses processos, a interoperabilidade de sistemas inserida intra e interorganizações, atrelada a utilização de protocolos gerais de

comunicação, como já visto, a exemplo do HTTP e SOAP; padrões de comunicação específicos da área da saúde, tais como: HL7, DICOM, TISS; padrões de sintaxe cujos principais representantes são o XML e o JSON; e padrões de documentação clínica: CDA, CCR, ISO (arquétipos), podem contribuir para a redução de riscos à saúde e melhoria no atendimento ao paciente.

Com as definições de interoperabilidade já apostas neste trabalho (ver item 1.3 do Capítulo 1), o sistema disponibiliza o acesso aos dados clínicos do paciente armazenados em diferentes locais de rede. Essa ferramenta está inserida no sistema utilizado pela saúde suplementar denominado Padrão TISS, que recepciona, através de códigos alfanuméricos, informações gerenciais de pacientes beneficiários.

Além do Padrão TISS, outros padrões foram escolhidos para maior aprofundamento neste trabalho (ver item 1.3 do Capítulo 1; item 2.1 do Capítulo 2) e, em sua grande maioria, pode-se dizer que apresentam alto nível de detalhamento em sua estrutura além de preencherem necessidades para qual se destinam.

A Classificação Internacional de Doenças, atualmente na versão 10, dando origem ao termo “CID10”, pode ser considerado um dos padrões mais conhecidos na área da saúde para a troca de dados. No Brasil, são exemplos a Tabela SUS (tabela de procedimentos, medicamentos e OPM[59] do Sistema Único de Saúde) e o TISS (Padrão para Troca de Informação na Saúde Suplementar).

A escolha do Padrão TISS no Capítulo 2 para ser explorado como padrão de comunicação em saúde, compreende diversos dos fatores isoladamente abordados, no entanto, leva ao entendimento de sua estrutura, conteúdo e finalidade.

Como um sistema padrão para trocas eletrônicas de dados entre os agentes de saúde suplementar, o Padrão TISS preconiza a interoperabilidade de sistemas de informação – que se mostra positiva na interação com demais plataformas de acesso e informações do paciente; entretanto, enfrenta vulnerabilidades de rede que pode comprometer a privacidade do titular – da Agência Nacional de Saúde (ANS).

A organização deste Padrão em 05 (cinco) componentes: (i) organizacional; (ii) conteúdo e estrutura; (iii) representação de conceitos em saúde; (iv) segurança e privacidade; e, (v) comunicação (ver item 2.2 do Capítulo 2), eleva o sistema para uma análise de pontos positivos:

---

[59] Órteses, Próteses e Materiais especiais.

1) Melhoria nos processos de administração da organização através da implantação de regras de uso;

2) Disponibilização de dados através do RES (Registro Eletrônico em Saúde) propiciando maior atenção à saúde do paciente;

3) Consolidação dos conceitos em saúde a partir do uso da Terminologia Unificada de Saúde Suplementar (TUSS).

4) Armazenamento em nuvem.

Relacionando cada indicativo acima para o contexto à proteção à privacidade no tratamento de dados pessoais dos titulares e, por vezes, usuários de planos de saúde, insta ressaltar que o Programa de Governança em Privacidade (PGP) – expressamente previsto pela LGPD – é ferramenta que auxilia na melhoria dos processos de administração e também propõe às organizações a criação de “planos de ação” para a gestão de dados, seja através de sistemas ou treinamentos de equipe técnica.

Isso porque, alinhado com a disponibilização de dados em RES, o Plano de Governança em Privacidade também é capaz de definir os mecanismos se segurança que serão utilizados para a gestão dos riscos e incidentes de segurança, buscando a redução da exposição ruídos à privacidade.

Diante de diversos processos a serem executados separadamente para complementar todo o Plano de Governança em Privacidade, sem sombra de dúvidas a padronização é o elemento chave e facilitador para abreviar as necessidades.

Prova disso a implementação do Padrão TUSS (ver item 1.3 do Capítulo 1) na atuação para uniformização das nomenclaturas médicas, colabora para a descrição precisa de dados e informações do paciente, além de criar celeridade para os procedimentos, desde o preenchimento do PEP até a contabilidade para tarefa do administrador responsável.

Por fim, o armazenamento de dados em nuvem computacional (ver o item 2.4 do Capítulo 2) favorece a agilidade em acesso às informações disponibilizadas em todos os processos elaborados pela clínica médica e hospitalar. Além disso, essa modalidade de armazenamento diferencia-se dos *softwares* locais por serem mais econômicos na implantação, agruparem com eficiência os recursos pretendidos e, principalmente, garantir amplo acesso à rede e a base de dados.

Como consequência, as plataformas de sistemas interoperáveis passam a tomar maior proporção em atuação, tornando-os acessos “possíveis” e, sem dúvida, agregando facilidades para a cadeia assistencial em saúde.

Inseridos no mesmo meio, é destacam-se também pontos negativos:

1) Troca eletrônica de informações a partir de padrões abertos, como o XML;

2) Utilização da chave HASH MD5 como ferramenta de “proteção” do dado registrado.

Os pontos negativos estão, em sua maioria, voltados a preocupação na tutela a privacidade do titular e dos dados pessoais expostos em prontuários armazenados com capacidade para acesso por meio de outros sistemas por envio de mensagem eletrônica.

A utilização de protocolos de saúde baseado em XML (ver item 2.2 do Capítulo 2) proporciona praticidade na descrição do dado e do entendimento universal, entretanto, é fator de preocupações pois esse modelo exige muito mais da segurança do sistema. Ou seja, para possibilitar a interoperabilidade entre diferentes sistemas a troca de dados de pacientes entre eles, a troca de dados é realizada a partir de uma rede sem fio, exposta a vulnerabilidades.

Ao longo da implementação do Padrão TISS, que entrou em vigor em 2012 por meio de Resolução Normativa nº 305, diversas adaptações foram sendo desenvolvidas para que as operadoras de planos de saúde buscassem conformidade e excelência no processo de informação à ANS.

Além de treinamentos exigidos para a manutenção do bom funcionamento do sistema, um dos pontos importantes para melhoria seria na remodelação no componente de segurança e privacidade, é a função *hash* criptográfica.

Funções *hash*, como MD5 ou SHA256, são funções que recebem como entrada uma cadeia de *bits* e geram uma saída de tamanho fixo (NIST, 2012). Essas funções são amplamente utilizadas para verificar a integridade de mensagens ou para assegurar a segurança de uma senha (HALDERMAN et al. 2005).

Ocorre que, comparando o *hash* MD5 com o *hash* SHA256 (MARTINEZ; DESTRO, 2014), objetivando o armazenamento de prontuários eletrônicos, foi verificado que ambas as funções criptográficas testadas apresentaram modificações. Com o resultado representado na Figura 10 é possível verificar que adulteração do

hash SHA256 apenas 3 (três) caracteres permaneceram na posição, enquanto no *hash* MD5 a quantidade de caracteres inalterável foi de 5 (cinco).

Prontuário	***SHA256***
Original	6716d425a0de9ff5871bfad6d819ed48 a95672da7c5c6bc39c8edd475df12269
Adulterado	4ace807c8aa556cccda71646f92382f3 99344e7ba1487631d62575e459a06fac
Prontuário	***MD5***
Original	2ab459a7b7e0cb50a6973e2d8a41dafc
Adulterado	98082c54b71289fbbb97ae3357086745

Figura 10: Comparação Hash MD5 e SHA256 (Fonte: MARTINEZ; DESTRO, 2014)

Martinez e Destro (2014) que realizaram o estudo representado pela figura acima, concluíram que a utilização do *hash* MD5 permite – com maior facilidade – a detecção de uma eventual fraude, comparado ao SHA256.

Logo, com o intuito de que os dados de beneficiários sejam rigorosamente armazenados com segurança, em razão da alta necessidade de resguardar à privacidade e intimidade do indivíduo, antes de haver a responsabilização dos agentes de tratamento, é interessante observar a possibilidade de adoção de outras medidas que podem se adequar ao contexto.

Como expressamente prevê a LGPD, inclusive como princípio da própria lei, a segurança do dado é condição irrefutável. Portanto, para adequação deste critério ao bom funcionamento do Padrão TISS, restou comprovado que a alteração da ferramenta de contenção de ameaças poderia ser substituída pela SHA256, a fim de agregar maior grau de sigilo ao ambiente virtual do qual a informação é armazenada e trocada.

Dessa forma, levando em consideração a proteção de dados e, em especial, a proteção de dados pessoais sensíveis, voltados para a troca de informações em sistemas eletrônicos interoperáveis utilizados na saúde suplementar, sob tutela da LGPD, resta inquestionável a reformulação do requisito de Segurança da Informação como fator primordial à preservação de direitos constitucionalmente inalteráveis.

2. CONCLUSÃO

Diante da pesquisa realizada, verificou-se que a preservação dos direitos personalíssimos dos titulares de dados pessoais se apresenta como tarefa desafiadora perante o compartilhamento de dados entre sistemas heterogêneos.

Na problemática dedicada em apresentar respostas sobre a vulnerabilidade da privacidade do titular e da integridade da mensagem no compartilhamento de dados entre diferentes interfaces, concluiu positivamente a hipótese levantada.

O trabalho dividido em 03 (três) capítulos, se organizou em abordar no Capítulo 1 sobre a construção dos fundamentos necessários para embasar a continuidade da pesquisa. Com a finalidade de construção de uma base teórica, neste capítulo foram analisadas as perspectivas de proteção aos direitos de privacidade e intimidade do titular de dados pessoais (elemento principal no desenvolvimento do trabalho) conforme disposição constitucional e demais legislações complementares que integram o sistema jurídico nacional. Ainda, desenvolveu as previsões contidas na Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709 de 2018 (LGPD), com enfoque à proteção específica aos dados de saúde (dados sensíveis) e às recomendações de boas práticas de segurança a serem adotadas na construção de sistemas operacionais.

O Capítulo 2 discorreu sobre a dinâmica dos dados dentro dos sistemas de saúde, em especial na saúde suplementar, tendo sido verificados elementos de segurança altamente frágeis com capacidade de exposição dos dados pessoais, consequentemente do titular.

Fez-se necessário, portanto, identificar os *assets* críticos de segurança. Utilizou-se para a análise 02 (dois) procedimentos adotados pela saúde suplementar: (i) o formato do Padrão TISS (Troca de Informações da Saúde Suplementar) e (ii) TUSS (Terminologia Unificada na Saúde Suplementar). Ambos inspirados no padrão internacional HL7 de comunicação em dados de saúde, tanto o TISS quanto o TUSS representam a adesão a padronização incorporada pelas operadoras privadas de planos de saúde que os utilizam com finalidade de comunicação e complementação de cadastros administrativos e de controle.

Em um primeiro momento, os dados de saúde trocados pelo TISS, mesmo que com a finalidade de gestão, não identificam seus titulares, porém, mediante a combinação com outras informações, o cenário permite torná-los identificáveis.

Ainda, foram apontados 02 (dois) fatores que integram o Padrão TISS e que podem ser causa da exposição do titular: (i) a verificação vulnerável de informações e (ii) a troca de dados sem o rigor de segurança devidamente exigido.

Da análise destes elementos verificou-se que: o TISS é um protocolo baseado em linguagem XML e, também, utiliza como garantia para a integridade dos dados o *hash* gerado a partir do algoritmo MD5.

Nesses cenários, ponderando a união de ambos em um único sistema, confirmou-se a fragilidade em termos de segurança do padrão TISS para o compartilhamento de dados entre sistemas, levando em consideração a troca de dados realizados em ambiente distribuído (XML) e a possibilidade de injeção de vetores que afetam a integridade da informação ao destinatário (*hash* MD5).

Por fim, o Capítulo 3, foi executado com o objetivo de indicar os elementos com a finalidade de remediar o surgimento de ameaças aos sistemas operacionais dos padrões em saúde, sugerindo a implementação de Programa de Governança em Privacidade (PGP) às operadoras de planos de saúde que fazem o uso do Padrão TISS, além da substituição da função criptográfica na estrutura deste padrão, alterando o *hash* MD5 para SHA256.

Os melhoramentos sugeridos contribuem para a formação de uma interface rígida com maior probabilidade de repelir o risco à exposição e violação dos direitos de privacidade e intimidade do titular, tornando o compartilhamento de dados pessoais e sensíveis uma operação em condições de segurança técnica favoráveis e propícias para a atuação de Sistemas de Informação (SI) de instituições clínicas e hospitalares, públicos ou privados, de modo a favorecer a troca entre os sistemas de saúde, sem esquecer da proteção de dados e, consequentemente, do titular de dados.

Assim, conclui-se que a integridade da mensagem compartilhada entre sistemas interoperáveis cuja a segurança esteja calçada em troca eletrônica de dados por meio de uma rede sem fio e, ainda, com compartilhamento de dados entre sistemas interoperáveis por meio de diferentes interfaces possa garantir a privacidade do titular, confirma-se a hipótese de pesquisa a partir da observância rigorosa dos *assets* de segurança físicos e operacionais dos sistemas que integram os padrões utilizados na saúde.

REFERÊNCIAS

ALMEIDA, Luiz Eduardo de. Governança Corporativa. In: VENTURINI, Otavio Venturini et al (Coord.). Manual de Compliance. Rio de Janeiro: Forense, 2019. p. 13.

ALQASSIM, Shamma; GANESH, Madhumeta; KHOJA,Shaheen; ZAIDI, Meher, 2016.

ARDENGHI, Régis Schneider. Direito à Vida Privada e Direito à Informação: Colisão de Direitos Fundamentais. Revista da ESMESC, Florianópolis, v. 19, n. 25, p. 227-251, 2012. Disponível em: https://revista.esmesc.org.br/re/article/view/57. Acesso em: 10 out. 2021.

ARMS, William Y. A spectrum of interoperability: the site for science for prototype for the NSDL. V. 8, n.1. 2002. Disponível em: http://www.dlib.org/dlib/january02/arms/01arms.html. Acesso em: 14 jul. 2021.

BEAL, Adriana. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

BIOCO, João. Segurança de dados na cloud computing: a survey. Universidade da Beira Interior. Covilhã – Portugal, 2016. Disponível em: file:///C:/Users/Bianca%20Amorim/Downloads/JoaoBioco_TAC_seguranca-de-dados_naCloud.pdf. Acesso em: 16 fev. 2022.

BIONI, Bruno R. Xeque-mate: o tripé da proteção de dados pessoais no jogo as iniciativas legislativas no Brasil. Disponível em: https://www.researchgate.net/publication/328266374_Xeque-Mate_o_tripe_de_protecao_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 1º jul. 2021.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BIONI, Bruno. Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BOFF, Salete Oro; FORTES, Vinicius Borges. A privacidade e a proteção de dados pessoais o ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. N. 68, p. 109-127. Florianópolis: Sequência, 2014.

BOFF, Salete Oro; FORTES, Vinicius Borges; FREITAS, Cinthia Obladen de Almendra. Proteção de dados e privacidade: do direito às novas tecnologias da sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. Agência Nacional de Saúde Suplementar – ANS. Padrão TIIS – Componente Organizacional. Disponível em: https://www.gov.br/ans/pt-br/arquivos/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-tiss/padrao-tiss/padrao-tiss-componente-organizacional-202106.pdf . Acesso em: 16 fev. 2022.

BRASIL. Agência Nacional de Saúde Suplementar – ANS. Resolução Normativa nº34 de 13 de fevereiro de 2009. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/ans/2009/int0034_13_02_2009.html . Acesso em: 11 out. 2021.

BRASIL. Agência Nacional de Saúde Suplementar – ANS. Resolução Normativa nº 153 de 28 de maio de 2007. Disponível em: https://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MTE4Mg== . Acesso em: 11 out. 2021.

BRASIL. Agência Nacional de Saúde Suplementar – ANS. Resolução Normativa nº 305 de 9 de outubro de 2012. Disponível em: https://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MjI2OA==. Acesso em: 20 jul. 2021.

BRASIL. Agência Nacional de Saúde Suplementar – ANS. Resolução Normativa nº 443 de 25 de janeiro de 2019. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/60739749/do1-2019-01-28-resolucao-normativa-rn-n-443-de-25-de-janeiro-de-2019-60739541 Acesso em: 07 dez. 2021.

BRASIL. Conselho Federal de Medicina. Cartilha sobre: “prontuário eletrônico: a certificação de sistemas de registro eletrônico de saúde”. Câmara Técnica de Informática em Saúde. Brasília – DF, 2012. Disponível em:

http://www.sbis.org.br/certificacao/Cartilha_SBIS_CFM_Prontuario_Eletronico_fev_2012.pdf. Acesso em: 07 out. 2021.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm Acesso em: 13 dez. 2021.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2011]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 out. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 6 out. 2021.

BRASIL. Lei nº12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para a formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm . Acesso em: 1 ago. 2021.

BRASIL. Lei nº12.737, de 30 de novembro de 2012. Dispõe obre a tipificação criminal de delitos informáticos; altera o Decreto Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 27 set. 2021.

BRASIL. Ministério da Saúde. Gabinete do Ministro. Portaria nº 188, de 3 de fevereiro de 2020. Declara Emergência em Saúde Pública de importância Nacional (ESPIN) em decorrência da Infecção Humana pelo novo Coronavírus (2019- nCoV). Brasília, DF:

Luiz Henrique Mandetta, 2020, Disponível em: https://www.planalto.gov.br/ccivil_03/portaria/portaria-188-20-ms.htm. Acesso em: 27 set. 2021.

BRASIL. Ministério da Saúde. Portaria nº2.073, de 31 de agosto de 2011. Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar. Brasília – DF, Ministro de Estado da Saúde. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html. Acesso em: 07 out. 2021.

BRASIL. Superior Tribunal de Justiça. Súmula nª 550. Recurso Especial 1.304.736/RS, Rel. Brasília, DF: Ministro Luis Felipe Salomão, Segunda Seção, julgado em 24/02/2016.

BRAVO, Roger. Segurança da Informação, CiberSegurança e CiberCrime: contributos para um alinhamento de conceitos. v.12. Lisboa, 2021. Disponível em: file:///C:/Users/Bianca%20Amorim/Downloads/Seguranca_da_informacao_e_ciberseguranca%20(1).pdf. Acesso em: 31 mai. 2021.

BRINEY, Kristin. Data management for researchers: organize, maintain and share your data for research success. Exeter, UK: Pelagic Publishing, 2015.

CAMPOS, V.F. Qualidade Total: padronização de empresas. Belo Horizonte, Fundação Cristiano Ottoni, 1992.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. Sequência: Estudos Jurídicos e Políticos, Florianópolis, v. 38, n. 76, p. 213-240, set. 2017. ISSN 2177-7055. Disponível em: https://doi.org/10.5007/2177-7055.2017v38n76p213. Acesso em: 25 out. 2021.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em Informática e de Informações – São Paulo: Editora SENAC São Paulo, 1999.

CHRISTEL, Michael G.; KANG, Kyo C. Issues In Requirements Elicitation. Technical Report CMU/SEI- 92-TR-12, Software Engineering Institute, Carnegie Mellon University, 1992.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 2.228, de 26 de fevereiro de 2019. Revoga a resolução CFM nº 2.227, publicada no D.O.U. de 6 de fevereiro de 2021.

CORTEZ, Igor Siqueira; KUBOTA, Luiz Cláudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. Revista de Administração de São Paulo. V.48, n.4, p. 757-769. São Paulo, 2013.

CRUZ, Márcio Freire. Servidor HL7-OPC para aquisição e integração de sinais vitais de pacientes em motorização clínica. Dissertação Mestrado Universidade Federal da Bahia. Escola Politécnica. Salvador, 2015.

DA SILVA NETTO, Abner; SILVEIRA, Marco Antônio Pinheiro. Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas. V. 4, nº 3. P. 375-397. Revista de Gestão a Tecnologia e Sistemas da Informação, 2007. Disponível em: https://www.scielo.br/j/jistm/a/Vx8Ypv6mDjxdYkKKrfYVgqz/?lang=pt&format=pdf. Acesso em: 26 jul. 2021.

DE FLÔRES, Mariana Rocha; SILVA, Rosane Leal. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. Revista de Direito. Vol. 12. N. 02. ISSN 2527-0389. Viçosa, 2020.

DE HOLANDA, Maristela Terto; FERNANDES, Jorge H.Cabral. Segurança no desenvolvimento de aplicações. Brasília, 2011. 43p.

DE MORAES, Maria Celina Bodin; DE QUEIROZ, João Quinelato. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. IN: Cadernos Adenauer, volume 3, Ano XX, 2019.

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

DISTERER, Georg. ISO/IEC 27000,27001 and 27002 for Information Security Management. Journal of Information Security. Scientific Research. Abril, 2013. Disponível em: https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf . Acesso em: 24 set. 2021.

DOD JP1-02. Department of Defense Dictionary of Military and Associated Terms (As Amended Through 15 August 2012). Vol.2010. Joint Publication 1-02. Disponível em: https://irp.fas.org/doddir/dod/jp1_02.pdf. Acesso em: 11 out. 2021.

DONEDA, Danilo. A proteção de Dados Pessoais como um Direito Fundamental. Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 22 mai. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. V. 12, n. 2, p. 81-108. Joaçaba: Espaço Jurídico, 2011.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos de formação da lei geral de proteção de dados. São Paulo: Thompson Reuters Brasil, 2019.

ELER, Kalline C. G. A releitura da privacidade: do “direito de ser deixado só” ao direito de autodeterminação informativa. V. 5, n.2. Espanha, 2016.

FONTES, Edison. Políticas e normas para segurança da informação. Rio de Janeiro: Brasport, 2012. p. 17-22.

UNIÃO EUROPEIA. GDPR – General Data Protection Regulation. Regulamento nº 2016/679. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679. Acesso em 27 set 2021.

GOMES, Fabio Guedes. Conflito social e welfare state: estado e desenvolimento social no Brasil. Fls. 201 a 236. vol.40 n.2. Rio de Janeiro: Revista de Administração Pública, 2006.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, Término do tratamento de dados, IN: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoais, Editora RT: São Paulo, 2019.

HINTZBERGEN, Jule; SMULDERS, André; BAARS, Hans; HINTZBERGEN, Kees. Fundamentos de segurança da informação, com base a Isso 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

HOEPERS, Cristiane. Princípios de segurança da informação. I Ciberjur. São Paulo: OAB. Recuperado em 7 fevereiro, 2012, de http://www.cert.br/docs/palestras/ certbr-ciberjur2011.pdf. Acesso em: 27 set. 2021.

INDARTE, S.; GUTIERREZ P.P. Estándares e interoperabilidad en salud electrónica: requisitos para una gestión sanitaria efectiva y eficiente. Santiago do Chile: CEPAL (ONU), 2011.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. Information security governance: guidance for boards of directors and executive management. Illinois: Rolling Meadows, 2001.

INTERNATIONAL ASSOCIATION FOR DEVELOPMENT OF THE INFORMATION SOCIETY (IADIS). E-Society 2004. V.1. Anais da Conferência Internacional IADIS. Ávila-ES, 2004. Disponível em: https://www.researchgate.net/profile/Piet-Kommers-2/publication/323277298_E-Society_2004_Vol1/links/5a8b9b98a6fdcc6b1a43de87/E-Society-2004-Vol1.pdf#page=500. Acesso em: 14 out. 2021.

ISO 13606-1:2008. Informática em saúde – Comunicação de prontuário eletrônico – Parte 1: Modelo de referência. Disponível em: https://www.iso.org/standard/40784.html. Acesso em: 11 out. 2021

ISO 13606-2:2019. Informática em saúde – comunicação de registro eletrônico de saúde – Parte 2: especificação de intercâmbio de arquétipos. Disponível em: https://www.iso.org/standard/62305.html. Acesso em: 11 out. 2021.

ISO/TR 20514:2015. Informática em saúde – Registro Eletrônico de Saúde – Definição, escopo, contexto. Disponível em: https://www.iso.org/standard/39525.html. Acesso em: 11 out. 2021.

JANNUZZI, C. A. S. C. Informação tecnológica e para negócios no Brasil: conceitos e terminologias. 1999. 139f. Dissertação (Mestrado em Biblioteconomia e Ciência da Informação) – Pontifícia Universidade Católica, Campinas, 1999.

LEMOS, André; LÉVY, Pierre. O futuro da Internet: em direção a uma ciberdemocracia planetária. São Paulo: Paulos, 2010

LYRA, Mauricio Rocha. Governança da Segurança da Informação. Brasília, 2015. ISBN: 978-85-920264-1-7

MACHADO, Joana de Moraes Souza. A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil. Porto Alegre, RS: Editora Fi, 2018. E-book. Disponível em: https://www.editorafi.org/494joana. Acesso em: 12 out. 2021.

MAGRANI, Eduardo. Entre dados e robôs: ética e privacidade na era da hiperconectividade. Rio de Janeiro: Konrad Adenauer Stiftung, 2018.

MARTINEZ, Gabriel Tamassia; DESTRO, Ricardo de Carvalho. Prontuário eletrônico com estrutura centralizada de assinatura eletrônica. Centro Universitário FEI. São Bernardo do Campo, São Paulo, 2014. Disponível em https://fei.edu.br/70anos/simposio/trabalhos2014/eletrica/gabriel_tamassia_martinez_ricardo_destro.pdf. Acesso em: 10 dez. 2021.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. Uma metodologia para a implantação de um sistema de gestão de segurança da informação. V. 2, n. 2. São Paulo: Revista de Gestão da Tecnologia e Sistema da Informação, 2005. p. 121-136.

MARTINS, Guilherme Magalhães; TELES, Carlos André Coutinho. A telemedicina na saúde suplementar e a responsabilidade civil do médico no tratamento de dados à luz da LGPD. Revista Estudos Institucionais (REI), v. 7, n. 1, p. 182-197, abr. 2021. ISSN 2447-5467. Disponível em: https://estudosinstitucionais.com/REI/article/view/608 . Acesso em: 31 jan. 2022.

MARTINS, Patricia Helena; TOMÉ, Bruna Borghi; PEGAS, Carolina Vargas. Relações de consume e as excludentes de responsabilidade civil na LGPD. Revista Consultor Jurídico, 1 junho de 2021. Disponível em: https://www.conjur.com.br/2021-jun-01/opiniao-excludentes-responsabilidade-civil-lgpd. Acesso em: 29 nov. 2021.

MATTSSON, M. Object-oriented Frameworks - A survey of methodological issues, Licentiate Thesis, Department of Computer Science, Lund University, CODEN: LUTEDX/(TECS-3066)/1-130/(1996), also as Technical Report, LU-CS-TR: 96-167, Department of Computer Science, Lund University, 1996.

MAZIERO, Carlos Alberto. Sistemas operacionais: conceitos e mecanismos (recurso eletrônico). Universidade Federal do Paraná (UFPR). Curitiba, 2019. Disponível em: http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=socm:socm-00.pdf. Acesso em: 28 set. 2021.

MÉDICI, André. Registros eletrônicos em saúde: uma ferramenta a favor a Universalização da Transparência. Ano 5, nº 13. Maio, 2010. Disponível em: http://monitordesaude.blogspot.com/2010/05/registros-eletronicos-de-saude-uma.html Acesso em:13 out. 2021.

MELL, Peter; GRANCE, Tim. *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology, vol. 53, p. 50, 2012.

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, v. 120, 2018.

MIKLE, Ondrej. Pratical attacks on digital signatures using MD5 message digest. Department of Software Engineering at Faculty of Mathematics and Physics. Charles University at Prague, Czech Republic. Dez.2004.

MILLER, Paul. Interoperability. What is it and why should I want it? United Kingdon: UKOLN, 2000. http://www.ariadne.ac.uk/issue/24/interoperability/ Acesso em: 14 jul. 2021.

MORENO, Ramon Alfredo. Interoperabilidade de Sistema de Informação em Saúde. Journal of Health Informatics. Julho-Setembro, 2016. Disponível em: http://www.jhi-

sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/viewFile/502/268. Acesso em: 13 out. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. Revista de Direito e Garantias Fundamentais. Edição Temática: Estado de Direito e Tecnologia. V.19. n.3. p. 159-180. Set/dez de 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf. Acesso em: 21 set. 2021.

OPENEHR. *Open industry specifications, models nd software for e-health*. Disponível em: https://www.openehr.org/about/what_is_openehr. Acesso em: 15 jul. 2021.

ORGANISATION FOR ECONOMIC CO-OPERATIONAND DEVELOPMENT. Civil Society and the OECD. Paris, 2002. Disponível em: https://www.oecd.org/. Acesso em: 14 out. 2021.

ORGANISATION FOR ECONOMIC CO-OPERATIONAND DEVELOPMENT. Eletronic commerce. Paris, 2001. Disponível em: https://www.oecd.org/. Acesso em: 14 out. 2021.

ORGANISATION FOR ECONOMIC CO-OPERATIONAND DEVELOPMENT. Issues related to security of information systems and protection of personal data and privacy. Paris, 1996. Disponível em: https://www.oecd.org/ Acesso em: 14 out. 2021.

ORGANISATION FOR ECONOMIC CO-OPERATIONAND DEVELOPMENT. Reporto on the OECD fórum session on the privacy-enhandling technologies. Paris, 2001. Disponível em: https://www.oecd.org/. Acesso em: 14 out. 2021.

Organização Mundial da Saúde (OMS). OMS Director-General's statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV). Geneva: WHO; 2020. [cited 2020 Apr 16]. Available from: https:// www.who.int/news-room/detail/23-01-2020-statement-on-the-meeting-of-the-international-healthregulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov)

PASQUAL, Juliana; SUNYE, Marcos. Uso de XML para interoperabilidade entre bases heterogêneas. V.2, n.1. Instituto Brasileiro de Estudos e Pesquisas Sociais: Revista Eletrônica de Sistemas de Informação, 2003.

PEMBLE, M. What do we mean by “information security”. Computer fraud and security, v.2004, n.5, p.17-19. May. 2019.

PEREIRA, Francisco R. F; GUEDES, Elloá B.; ASSIS, Francisco M. Protocolo para autenticação quântica de mensagens clássicas utilizando variáveis contínuas. XXXIII Simpósio Brasileiro de Telecomunicações. Juiz de Fora – MG: 2015. Disponível em: file:///C:/Users/Bianca%20Amorim/Downloads/Protocolo_para_Autenticacao_Quantica_de_Mensagens_.pdf. Acesso em: 28 set. 2021.

RAMINELLI, Francieli Puntel; RODEGHERI, Leticia Bodanese. A proteção de dados pessoais a Internet o Brasil: análise de decisões proferidas pelo Supremo Tribunal Federal. V.11, n.2. Porto Alegre: Cadernos do Programa de Pós-Graduação m Direito, 2016.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). 10 FERREIRA, Ricardo et al, Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia, 2016. Acesso em: 10 ago. 2021.

RIBEIRO, Carlos Henrique Calazans; HIRA, Adilson Yuuji; ZUFFO, Marcelo Knorich. Aplicação da técnica de duplo hash na implementação de serviços de integridade em Registros Eletrônicos de Saúde. Laboratório de Sistemas Integráveis da Universidade de São Paulo. São Paulo, 2006. Disponível em: https://www.researchgate.net/profile/Marcelo-Zuffo/publication/266606943_Aplicacao_da_Tecnica_de_Duplo_Hash_na_Implementacao_de_Servicos_de_Integridade_em_Registros_Eletronicos_de_Saude/links/545bb1890cf2f1dbcbcafff4/Aplicacao-da-Tecnica-de-Duplo-Hash-na-Implementacao-de-Servicos-de-Integridade-em-Registros-Eletronicos-de-Saude.pdf Acesso em: 11 out. 2021.

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RONCHI, Daiane C. M.; SPIGOLON, Dandara N.; GARCIA, Diego; CICOGNA, Paulo E. S. L; BULEGON, Hugo; MORO, Claudia M. C. Desafios no desenvolvimento de prontuários eletrônicos baseados em arquétipos: avaliação fisioterapêutica funcional. Disponível em: https://www.scielo.br/j/fm/a/L3zxr4bnyS4ZpfchBQrFdvg/?lang=pt . Acesso em: 15 jul. 2021.

RUBÍ, Jesus Noel Suárez. Plataforma para m-Health baseada no Padrão OpenEHR, em Comunicações M2M e em Computação em Nuvem. Dissertação de Mestrado em Engenharia Elétrica. Publicação em PPGEEDM – 637/2016, Departamento de Engenharia Elétrica, Universidade de Brasília, DF, 2016. Disponível em: https://repositorio.unb.br/bitstream/10482/21561/1/2016_Jes%C3%BAsNoelSu%C3%A1rezRub.pdf. Acesso em: 5 nov. 2021

SALDAÑA, M. N. The right to privacy. Le génesis de la protección demla privacidad em el sistema constitucional norteamericano: el centenário legado de Werren y Brandeis, Revista de Derecho Político, n. 85, p. 195-240, 2012.

SALDANHA, Jânia Maria Lopez; BRUM, Márcio Morais; MELLO, Rafaela da Cruz. As novas tecnologias da informação e comunicação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. Anu. Mex. Der. Inter, México, v. 16, p. 461-498, dic. 2016. Disponível em: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542016000100461&lng=es&nrm=iso . Acesso em: 16 jun. 2021.

SALES, Odete Máyra Mesquita; PINTO, Vinginia Bentes. Tecnologias digitais de informação para a saúde: revisando padrões de metadados em foco na interoperabilidade. Ceará: Rev Eletron Comun Inf Inov Saúde, 2019. Disponível em: file:///C:/Users/Bianca%20Amorim/Downloads/1469-6808-1-PB%20(2).pdf. Acesso em: 14 jun. 2021

SANT´ANNA, Ricardo C. Gonçalves. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. Informação e Informação, Londrina, v. 21, n. 2, p. 116-142. Mai./Ago., 2016.

SANTANA, Ricardo César Gonçalves. Ciclo de Vida dos Dados e o Papel da Ciência da Informação. XIV Encontro Nacional de Pesquisa em Ciência da Informação (Enancib 2013), p. 21, [s.d.], 2013.

SARLET, Ingo Wolfgang. As dimensões da dignidade da pessoa humana: construindo uma compreensão jurídico-constitucional necessária e possível. In: SARLET, Ingo Wolfgang (Org.). Dimensões da Dignidade: Ensaios de Filosofia do Direito e Direito Constitucional. Porto Alegre, RS: Editora Livraria do Advogado, 2013.

SAYÃO, Luiz Fernandes; MARCONDES, Henrique. O desafio da interoperabilidade e as novas perspectivas para as bibliotecas digitais. V. 20, n. 2, p.133-148. Campinas: TransInformação, 2008. Disponível em: https://brapci.inf.br/index.php/res/download/118043 . Acesso em: 14 jul. 2021

SILVA, Rosane Leal da. As tecnologias da informação e comunicação a proteção de dados pessoais. Anais do XIX Encontro Nacional do CONPEDI. Fortaleza: jun. 2010. Disponível em: https://s3.amazonaws.com/conpedi2/anteriores/XIX+Encontro+Nacional+-+UFC-Fortaleza+(09%2C+10%2C+11+e+12+de+junho+de+2010).pdf. Acesso em: 30 jun. 2021.

SINGH, Simon. “The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography”. Nova Iorque: Anchor Books, 1999.

SOLOVE, Daniel J. I've Got Nothing to Hide and Other Misunderstandings of Privacy. San Diego Law Review, San Diego, v. 44, p.759, jan. 2007. Disponível em: acesso em: 28 set. 2018. p. 759

SOUSA, Flávio R. C.; MOREIRA, Leonardo.; MACHADO, Jarvam C.. Computação em Nuvem: Conceitos, Tecnologias, Aplicações e Desafios. Ceará, 2010. Disponível em: https://www.researchgate.net/publication/237644729_Computacao_em_Nuvem_Conceitos_Tecnologias_Aplicacoes_e_Desafios Acesso em: 27 jul. 2021

STALLINGS, William; BROWN, Lawrie. Segurança e Computadores 2.ed. Elsevier Editora Ltda, Rio de Janeiro, 2014, Acesso em: 27 jul. 2021

TELES, Guilherme. O que é o NIST CyberSecurity Framework? Disponível em: https://guilhermeteles.com.br/o-que-e-o-nist-cybersecurity-framework/ . Acesso em: 02 jun. 2021.

TEPEDINO, Gustavo. O reconhecimento pelo STF do direito fundamental à proteção de dados. V. 24. P. 11-13. Belo Horizonte: Revista Brasileira de Direito Civil – RBDCivil, 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/587/358. Acesso em: 02 jun. 2021.

TEPEDINO, Gustavo; DE TEFFÉ, Chiara Spadaccini. O consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil – RBDCivil. Belo Horizonte, v. 2, p. 83-116. Jul/Set, 2020. Disponível em: file:///C:/Users/Bianca%20Amorim/Downloads/521-1918-1-PB.pdf. Acesso em: 1º dez. 2021.

UKOLN. Interoperability focus: looking at interoperability, 2005. Disponível em: http://www.ukoln.ac.uk/interop-focus/about/flyer-interoperability.pdf Acesso em: 14 jul. 2021.

VALE, Sávio. Definição, funcionamento e as aplicações do hash, a função popular da criptografia. (2020). Disponível em: https://www.voitto.com.br/blog/artigo/o-que-e-hash-e-como-funciona . Acesso em: 10 dez. 2021.

VARIAN, H. (2004). *System reliability and free-riding*. In L. J. Camp, & S. Lewis (Eds.). Economics of Information Security. Advances in Information Security, 12, pp. 1-15. New York: Springer. doi: 10.1007/1-4020-8090-5_1. Acesso em: 27 set. 2021

WADLOW, Thomas A. Segurança de Redes. 1ªEd. Editora Campus, 2000.

WARREN, Samuel D.; BRANNDEIS, Louis D. The right to privacy. Harvard Law Review, vol. IV, n. 5, 1890. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html . Acesso em: 02 set. 2021.

WILLIAMS, P. Information security governance. Information security technical report. V. 6, n.3., p. 60-70. Nov.,2021.