INTERNATIONAL SYMPOSIUM ON TECHNOLOGICAL INNOVATION
ISTI 10 YEARS
SEPTEMBER 25TH TO 27TH, 2019
ARACAJU, SERGIPE, BRAZIL

Inovação Tecnológica na Saúde: A Proteção de Dados Sensíveis na Telemedicina

Technological Innovation in Health Sistem: The Protection of Patient Medical Information at Telemedicine

George Geraldo Gomes de Magalhães - georgemagalhaes73@yahoo.com.br
Faculdade UNINASSAU (Campus: Petrolina, PE) – Departamento de Direito
Discente do Mestrado Profissional em Propriedade Intelectual e Transferência de Tecnologia para a Inovação – PROFINT (Ponto Focal: UNIVASF, Juazeiro, BA)

Resumo

A medicina brasileira culminou no processo de inovação tecnológica por meio da ferramenta denominada Telemedicina, desenvolvida para fins de encurtar distâncias e aproximar o médico do paciente, a qual disponibiliza ao mercado uma melhoria na eficiência e rapidez da prestação dos serviços médicos, acessível em qualquer localidade, por meio digital, porém a problemática mais evidente na tarefa diz respeito à proteção de dados sensíveis dos pacientes, os quais são compartilhados por meio do citado programa entre os profissionais da saúde, situação já regulamentada pelo Conselho Federal de Medicina, bem como acompanhada pelos conselhos estaduais de medicina. Em tema de produtos criados para fins de proteção de dados sensíveis de pacientes, analisa-se o teor de patentes de productos (softwares e hardwares) criados para tal finalidade, captadas das bases Quest Orbit, Espacenet e INPI. Os nossos tribunais superiores possuem jurisprudência favorável aos clientes/pacientes, ou seja, a parte vulnerável da relação entre planos de saúde e pacientes. Ademais, verifica-se ainda a análise de estudo de caso real, acerca de vazamento e compartilhamento de dados médicos de indivíduos, pela via digital, o que vem se tornando fato comum, ante ao crescente desenvolvimento das mídias sociais, as quais são utilizadas indevidamente por profissionais da saúde. Assim, o presente trabalho analisou dados de várias fontes e objetos de estudo (legislações, jurisprudência, patentes e caso prático), de modo a formar um cenário completo do estado da questão atinentes á proteção de dados desde outras áreas, até o cerne da Telemedicina.

Palavras-chave: proteção de informações, histórico médico, dados sensíveis, telemedicina.

Abstract

Brazilian medicine culminated in the process of technological innovation through a tool called Telemedicine, developed to shorten distances and bring the patient closer to the doctor, which provides the market with an improvement in the efficiency and speed of medical services, accessible in any location , by digital means, but the most evident problem in the task concerns the protection of sensitive data of patients, which are shared through the program among health professionals, a situation already regulated by the Federal Council of Medicine, as well as accompanied by the state councils of medicine. In terms of products created for the protection of sensitive patient data, the content of software patents (software and hardware) created for this purpose, captured from Quest Orbit, Espacenet and INPI databases.. Our courts have favorable jurisprudence for clients / patients, that is, the vulnerable part of the relationship between health plans and patients. In addition, it is also verified the analysis of a real case study, about leakage and sharing of medical data of individuals, by digital means, which has become common fact, before the growing development of social media, which are used improperly by health professionals. Thus, the present study analyzed data from various sources and objects of study (legislation, jurisprudence, patents *and case study), in order to provide a complete scenario of the state of the issue regarding data protection from other areas, to the core of Telemedicine.*

Keywords: information protection, medical historic, sensitive data, telemedicine.

1.Introdução

A sociedade contemporânea, denominada de sociedade de informação ou sociedade de rede, a qual é construída sob uma estrutura social com fulcro e manejada por tecnologias de comunicação que geram, processam e dividem informações acumuladas nas redes de computadores, a qual encontra-se em constante necessidade de troca de informações de forma rápida e por meio digital (MALDONADO; BLUM, 2019)

A proteção de dados da pessoa física é tema de ordem mundial, no qual diversos países já sancionaram leis específicas acerca do tema em discussão, como por exemplo: Argentina (Ley 25.326), Chile (ley 19.628), Brasil (Lei 13.709) e no âmbito da União Europeia, Portugal (Regulamento UE 2016/679), o que possibilitou a regulamentação quanto ao manejo, tratamento, compartilhamento e salvaguarda de dados de diversas áreas da vida do agente (pessoal, comercial, saúde etc.

No Brasil, vem ocorrendo diversas iniciativas no processo de desenvolvimento da telemedicina, como por exemplo o Programa Telessaúde Brasil, a Rede Nacional de Ensino e Pesquisas e a Rede Universitária de Telemedicina, e mais, com foco na atenção primária o Ministério da Saúde instituiu desde o ano de 2007 o Programa Nacional de Telessaúde, o qual foi ampliado no ano de 2011, conforme asseverado por Maldonado (2016), pois o Brasil é um país que oferece oportunidades ímpares para o desenvolvimento e as aplicações da telemedicina ante a sua grande extensão territorial.

Dentre as várias inovações tecnológicas ocorridas e elencadas nas referidas normas, verifica-se a criação de um sistema, em paralelo, que visa aproximar pacientes e profissionais de saúde (médicos), no sentido de levar aos mais distantes ou carentes municípios da Federação a possibilidade de uma consulta médica ou outros tipos de intervenções médicas, tudo por meio de uma ferramenta tecnológica denominada de Telemedicina[1], a qual já foi também regulamentada pelo Conselho Federal de Medicina – CFM por meio da Resolução CFM n. 2.227/2018[2].

Ademais, nesse cenário, podemos além da questão de compartilhamento de informações entre paciente e médico, verificar a existência de outras questões que circundam o tema, ou seja, em matéria constitucional quanto ao direito à privacidade (Sarlet, 2016) e proteção de dados ou informações denominadas de sensíveis, extraídas e anotadas (prontuário) pelo profissional da medicina, as quais merecem especial tratamento e proteção, pois do contrário poderão trazer implicações civis e penais aos responsáveis pelo vazamento ou exposição do paciente.

A referida exposição, de forma desnecessária ou negligente, pode trazer à luz informações as quais o paciente deseje sigilo delas, pois podem prejudicá-lo na esfera pessoal, profissional e/comercial.

Conforme Feigelson e Albani Siqueira (2019), apesar da existência de diversas leis em torno de vários países, como citado, bem como a existência de outras normas que tratam do instituto da proteção de dados, no âmbito bancário (sigilo bancário), do consumidor, a lei mais atual no tema em tela, em nosso país, diz respeito justamente à proteção de dados, promulgada no ano de 2018, trazendo à luz a preocupação com a manipulação, controle, compartilhamento e proteção de informações, inclusive as médicas, as quais detém natureza e caráter sensivelmente intimista do ser humano, que podem ser de grande valia sua captação irregular ou ilegal por terceiros.

Portanto, o presente trabalho tem o condão de analisar as implicações da lei de proteção de dados (lei 13.709) no cenário de atuação médica, em específico, na tarefa denominada TELEMEDICINA, no que tange as implicações jurídicas (constitucionais e legais) da proteção, bem como do vazamento de dados sensíveis de pacientes, de bancos de dados públicos ou privados e levantamento de sistemas criados para fins de proteção de dados, por meio de patentes existentes no mundo e no Brasil, realizada nos sistemas *Quest Orbit*, *Espacenet* e INPI e a visão dos tribunais superiores, por meio da análise de jurisprudência dos tribunais superiores (STJ e STF), tudo para se apresentar uma visão completa acerca do assunto.

2.Fundamentação teórica

[1] Consiste no uso das tecnologías de informação e comunicação na saúde, viabilizando a oferta de serviços ligados aos cuidados com a saúde, especialmente nos casos em que a distancia é um fator crítico. O termo telemedicina aparece na literatura como sendo ainda: telessaúde ou *e-saúde*.

[2] Portal.cfm.org.br

A transformação digital no setor da saúde é uma realidade incontornável e tem conhecido nos últimos anos, um crescimento exponencial, a nível mundial e nacional (Maldonado, Blum, 2019; Feigelson, Albani Siqueira, 2019). De fato, constata-se hoje um crescimento considerável tanto na oferta, pelo lado dos hospitais, clínicas, profissionais de saúde (médicos) e planos de saúde, como da procura, por parte dos pacientes, de produtos e serviços tecnológicos e digitais no setor de saúde (pública e privada).

Associado a essa revolução digital, surgem naturalmente preocupações ao nível da segurança dos dados sensíveis dos pacientes, privacidade e proteção dos dados utentes, em especial, os dados e informações do histórico clínico do indivíduo (Resolução CFM 2.227/2018).

Percebe-se que no mundo e no Brasil o tema proteção de dados já é um antigo conhecido do cenário jurídico, com diversas legislações publicadas, porém de forma difusa e a não contemplar de forma pontual a proteção dos dados do âmbito da saúde, que possuem importante repercussão na vida pessoal, profissional e comercial do indivíduo, caso sejam manejados de forma indevida (MENDES, 2014).

Schwab (2016) aponta que as mudanças produzidas pela conectividade digital em nossa sociedade atual e até o ano de 2025, geram aspectos positivos e negativos, ressaltando-se que os pontos negativos dizem respeito justamente a perda de privacidade, constante vigilância e diminuição da segurança de dados.

Nesse sentido, no cenário regional do Mercosul (Argentina, Chile, Uruguai etc.), Portugal (Europa) e no Brasil, percebe-se a existência de normas atinentes à proteção de dados, porém recentemente, em consonância com a preocupação acerca da proteção de dados sensíveis de pacientes, o Conselho Federal de Medicina – CFM exarou a Resolução CFM n. 2.227/2018, para disciplinar de modo pontual e específico o manuseio, tratamento, compartilhamento e guarda de informações sobre pacientes, que digam respeito a seu histórico de saúde, as quais são de interesse público e especialmente de entes privados, ou seja, planos de saúde.

3.Metodologia

O presente trabalho se desenvolverá por meio da metodologia de análise dos seguintes objetos de estudo: a) bibliográfico; b) patentes, e; c) estudo de caso. Terá como escopo temporal o lapso máximo de 20 (vinte) anos no que tange as legislações elencadas e analisadas, bem como de 10 (dez) anos para a bibliografia e patentes e como fonte de estudo bibliografia formalizada por livros, artigos científicos e legislação (nacional e estrangeira), bem como a busca e análise de patentes de produtos (sistemas de proteção de dados) realizadas nas bases: *Quest Orbit, Espacenet* e INPI.

4.Discussão e resultados

A preocupação com a proteção de dados do indivíduo, seja ele pessoa física ou jurídica, não é novidade no sistema jurídico nacional, pois antes mesmo da promulgação da Lei 13.709, já existiam outros instrumentos legais que disciplinavam a matéria, porém de uma forma difusa, sem especificidade, as quais buscavam a proteção de dados dentro da sua própria disciplina, ou seja, no âmbito das relações de consumo, no âmbito bancário e fiscal e outros (Marco Civil da Internet, *Habeas Data*, Lei de Cadastro Positivo etc.).

Dessa forma, pode-se exemplificar:

> **Constituição Federal de 1988. Art, 5º, X e XII**:
> "X - 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;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".
>
> **Habeas Data**:
> "Art. 7° Conceder-se-á *habeas data*:
>
> I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público;

II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável".

Código de Defesa do Consumidor:

Art. 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor".

Lei do Cadastro Positivo (Lei 12.414):

"Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
§ 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado".
Marco Civil da Internet:

"Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais".
Lei 12.527:

"Art. 4º Para os efeitos desta Lei, considera-se:

IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido".

Assim, comprova-se que a normatização acerca do amplo tema em análise não é novidade, porém se fazia necessário a regulamentação específica quanto a determinadas áreas, inclusive a de saúde, no tratamento, compartilhamento e guarda de dados sensíveis da vida do agente, por isso a busca pela elaboração e consequente promulgação da Lei Geral de Proteção de Dados.

Por outro lado, pode-se apontar no cenário regional (Mercosul) e Portugal a existência das seguintes regulamentações:

Argentina (Ley 25.326)
Art. 8º: "*Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional*".

Chile (Ley 19.628)
Art. 7º: "*Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo*".

Portugal (Regulamento UE 2016/679)
Art. 1º: "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.o, n.o 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.o, n.o 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

Art. 35: "Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro".

Art. 45: "Sempre que o tratamento dos dados for realizado em conformidade com uma obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública, o tratamento deverá assentar no direito da União ou de um Estado-Membro ".

Art. 53: "As categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controle da qualidade, informação de gestão

e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública".

Uruguay (Ley 18.331)
Art. 1º: "*Derecho humano.- El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República*".

Art. 19: "*Datos relativos a la salud.- Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley*".

Em ato contínuo, verificou-se o nascimento da Telemedicina e sua posterior regulamentação pelo Conselho Federal de Medicina – CFM e demais conselhos da ciência médica, principalmente no que tange ao manejo e compartilhamento de informações médicas de pacientes, conforme se passa a analisar, na esfera específica da temática de proteção de dados na atividade médica com uso de tecnologia.

A proteção de dados sigilosos do paciente é um dever do médico em qualquer circunstância, salvo raras exceções previstas em lei, como no caso de doenças contagiosas de notificação compulsória. Algumas operadoras de saúde (planos de saúde) fazem uso dos dados acerca da saúde e tratamento de pacientes para impor restrições de coberturas e sanções sobre os médicos que prescrevem determinados tipos de procedimentos.

O Conselho Federal de Medicina – CFM levando em consideração a inovação na área médica, bem como o uso de novas tecnologias na atividade do profissional da medicina, exarou a Resolução CFM n. 2.227/2018, asseverando que as informações sobre pacientes identificado só podem ser transmitidas a outro profissional com prévia autorização/permissão do paciente, mediante livre consentimento e sob protocolos de segurança, inclusive definindo a Telemedicina como sendo 2º exercício da medicina mediado por tecnologias para fins de assistência, educação, pesquisa, prevenção de doenças e lesões e promoção de saúde".

Assim, a Telemedicina encontra-se regulamentada do art. 1º ao 7º da Resolução CFM n. 2.227/2018, fixando que a responsabilidade pela guarda e compartilhamento das informações sobre o paciente é do médico que o atendeu, em que, no ambiente moderno (digital) deve atender aos seguintes requisitos fundamentais: *a) a confidencialidade*[3]*; b) a integridade*[4]*; c) a disponibilidade*[5]*, e; d) a conformidade legal e normativa, nomeadamente a privacidade*[6].

No mesmo sentido, nas teleconsultas são obrigatórios os seguintes documentos: *a) identificação das prestadoras de serviço de saúde; b) termo de consentimento do paciente; c) identificação de dados do paciente; d) registro de data e hora do início e final do atendimento; e) identificação da especialidade médica que prestou o serviço; f) informação acerca do motivo da consulta; g) anotações clínicas; h) diagnóstico; i) decisão clínica e terapêutica; j) dados relevantes de exames complementares; l) identificação de encaminhamentos clínicos; m) relatório médico, e; n) encaminhamento ao paciente do relatório médico.*

[3] Significa que a informação está protegida contra o acesso ou exposição a entidades não autorizadas.
[4] Significa que a informação mantém todas as características definidas pelo seu responsável, incluindo o controle das alterações ao longo do seu ciclo de vida.
[5] Significa que a informação está disponível ao pessoal autorizado sempre quue for relevante, em um determinado contexto específico (interesse público etc.).
[6] De acordo com a Lei de Proteção de Dados, bem como a Resolução do CFM.

Tal sigilo é necessário, pois o paciente acredita que tudo que disser ao médico, ou seus exames revelarem, não será informado a terceiros. A garantia desse sigilo médico passou a ser ameaçado pelos interesses econômicos dos planos de saúde, que desejam saber mais sobre o paciente/cliente, para planejar a condução do seu negócio perante o paciente (hipossuficiente), pois a privacidade se trata verdadeiramente de um direito fundamental, protegido por nossa Constituição (Sarlet, 2016; Afonso da Silva, 2009), portanto, verifica-se que apesar da existência de legislação acerca da proteção de dados em vários países, como mencionado, necessita-se da proteção específica quanto a dados sensíveis na telemedicina, questão não abordada pontualmente pelos países relacionados no presente trabalho, a título exemplificativo.

4.1 Sistemas de proteção de dados em patentes

Visando verificar a existência de sistemas de proteção de dados, seja em áreas diversas ou especificamente na área de saúde, a nível mundial e brasileiro, realizou-se pesquisa em base de dados dos seguintes sistemas de patentes: *Quest Orbit*[7], *Espacenet*[8] e INPI[9], tendo como escopo as seguintes palavras-chave: "proteção de dados" e "sistema", obtendo-se o seguinte resultado:

Sistema	**Patente**	**Nacionalidade**
Quest Orbit	2012WO-IB50420	ESTADOS UNIDOS
Espacenet	US2019180272	ESTADO UNIDOS
INPI	BR112019002220-1 A2	BRASIL
INPI	BR102016026407-3 A2	BRASIL
INPI	PI9802324-1 A	BRASIL
INPI	PI9903403-4 A	BRASIL

Pois bem. Da busca verificou-se que a patente 2012WO-IB50420 (USA) diz respeito a um sistema específico consistente em um servidor, um terminal de usuário e um identificador para a área de saúde, criado para a proteção e acesso de forma segura de dados/informações médicas de pacientes nele armazenados, oriundos de registro médico eletrônico, efetuados em hospitais, clínicas e por profissionais médicos, com conteúdo de registros de consumo medicamento, receitas médicas, principalmente de pacientes com doenças crônicas ou idosos, o qual será disponível apenas ao paciente ou familiar com autorização.

Tal sistema é interligado com diversas bases (clínicas, hospitais e consultórios médicos) para fins de acesso (pesquisa de histórico médico) e alimentação de informações médicas a partir de novas consultas ou intervenções, de modo a possibilitar a todos os profissionais ou estabelecimentos hospitalares, o conhecimento do histórico do paciente para melhor condução do tratamento ou indicação de outro profissional (especialidade).

A referida ferramenta tem o acesso restrito por parte do paciente ou familiar autorizado, via *Token*, caso o paciente/titular fique incapacitado.

A patente US2019180272 (USA) diz respeito a um sistema de proteção de identidade, de registros financeiros de consumidor associado a um cartão de crédito ou débito, cujos dados foram armazenados na rede. Verifica-se que se trata de um sistema dirigido a informações com fito comercial, visando montar perfil de consumidor por meio de dados de consumo oriundos de compras efetuadas por meio de cartão (crédito ou débito), cujo interesse se dá por parte de Instituições Financeiras, de crédito ou bancos.

A patente BR112019002220-1 A2 (BR) é um sistema para controlar os dados de um usuário de redes de telecomunicações e método para controlar dados de um usuário de redes de telecomunicações, ou seja, trata-se de um sistema e método que controla a recopilação dos inúmeros dados que cada usuário gera em

[7] www.orbit.com
[8] https://worldwilde.espacenet.com
[9] www.inpi.gov.br

sua interação com as redes e serviços de telecomunicações, a disponibilização do usuário para o seu conhecimento, a administração de permissões seletivas a terceiros para valorização dos ditos dados, assim como a atuação sobre a rede e serviços com base nos ditos dados.

Percebe-se no caso em tela que se trata de um sistema de natureza de atuação na esfera de dados telefônicos, ou melhor, de elaboração de informações e proteção de dados de registro telefônicos.

A patente BR102016026407-3 A2 (BR) também diz respeito a um método, sistema, aparelho para acesso aos dados pessoais do consumidor, que é gerado quando o referido usuário está operando com um primeiro fornecedor de serviços, para uso de um segundo operador de serviços, mantendo a privacidade do consumidor. Verifica-se que se trata de outro produto para montagem de perfil de consumidor.

A patente PI9802324-1 A (BR) diz respeito a um sistema específico para a área de saúde, ou seja, um cartão magnético para arquivar dados pessoais de saúde de seu usuário, ou seja, as informações do histórico de atendimentos, informações médicas pessoais quanto a idade, tipo sanguíneo, doenças preexistentes (hipertensão, diabetes etc.), estão armazenadas no magnético do cartão, que é de uso restrito e pessoal do paciente.

A patente PI9903403-4 A (BR) é atinente também a um *smart card* de saúde para arquivar dados pessoais do paciente, com chip e fotografia, diferentemente do produto anterior, este é mais moderno pois apresenta um *chip* e fotografia, ou seja, itens de segurança mais robustos.

Portanto, verificou-se que das patentes exemplificadas, três delas, uma estrangeira e duas brasileiras são de produtos específicos para a proteção de dados na área de saúde, ou seja, na área da medicina, o que demonstra que o nosso país está, tanto em tema de legislação, quanto em tema de patentes (produtos) acompanhando as mudanças externas e demandas por serviços e produtos seguros, como já respaldado pelas normas (CDC, Marco Civil da Internet, Lei Geral de Proteção de Dados, etc.) e em especial pela Resolução do CFM (Telemedicina).

4.2 A proteção de dados nos tribunais superiores do Brasil (Jurisprudência)

Após a análise legal, de ordem nacional e estrangeira, bem como do índice de patentes quanto a temática objeto do presente trabalho, passa-se no presente momento a verificar como os tribunais superiores do Brasil, em especial o Superior Tribunal de Justiça – STJ e o Supremo Tribunal Federal – STF estão decidindo acerca da questão da proteção de dados do indivíduo, seja na esfera difusa (consumidor, bancário, fiscal etc.) ou na esfera singular de nosso estudo, que é o âmbito de proteção de dados no cenário da atividade médica.

Pois bem. O STF tem decidido quanto ao tema "proteção de dados" em diversas esferas de atuação jurídica, por exemplo, no que diz respeito ao princípio da transparência, aduzindo que:

> O interesse público deve prevalecer na aplicação dos Princípios da Publicidade e Transparência, ressalvadas as hipóteses legais. A divulgação de dados referentes aos cargos públicos não viola a intimidade e a privacidade, que devem ser observadas na proteção de dados de natureza pessoal[10].

Ainda, na celeuma atinente a proteção de dados fiscais do indivíduo:

> Ementa: DIREITO CONSTITUCIONAL. DIREITO TRIBUTÁRIO. HABEAS DATA. ARTIGO 5º, LXXII, CRFB/88. LEI Nº 9.507/97. ACESSO ÀS INFORMAÇÕES CONSTANTES DE SISTEMAS INFORMATIZADOS DE CONTROLE DE PAGAMENTOS DE TRIBUTOS. SISTEMA DE CONTA CORRENTE DA SECRETARIA DA RECEITA FEDERAL DO BRASIL-SINCOR. DIREITO SUBJETIVO DO CONTRIBUINTE. RECURSO A QUE SE DÁ PROVIMENTO. 1. O habeas data,

[10] STF: RE 766390 AgR, Relator(a): Min. RICARDO LEWANDOWSKI, Segunda Turma, julgado em 24/06/2014, PROCESSO ELETRÔNICO DJe-157 DIVULG 14-08-2014 PUBLIC 15-08-2014.

> posto instrumento de tutela de direitos fundamentais, encerra amplo espectro, rejeitando-se visão reducionista da garantia constitucional inaugurada pela carta pós-positivista de 1988. 2. A tese fixada na presente repercussão geral é a seguinte: "O Habeas Data é garantia constitucional adequada para a obtenção dos dados concernentes ao pagamento de tributos do próprio contribuinte constantes dos sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais." 3. O Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil, conhecido também como SINCOR, registra os dados de apoio à arrecadação federal ao armazenar os débitos e créditos tributários existentes acerca dos contribuintes. 4. O caráter público de todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações é inequívoco (art. 1º, Lei nº 9.507/97). 5. O registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto. (…) Registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto, causando-lhe dano ao seu direito de privacidade.(...) in José Joaquim Gomes Canotilho, Gilmar Ferreira Mendes, Ingo Wolfgang Sarlet e Lenio Luiz Streck. Comentários à Constituição. Editora Saraiva, 1ª Edição, 2013, p.487. 6. A legitimatio ad causam para interpretação de Habeas Data estende-se às pessoas físicas e jurídicas, nacionais e estrangeiras, porquanto garantia constitucional aos direitos individuais ou coletivas. 7. Aos contribuintes foi assegurado constitucionalmente o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente, verbis: Art. 5º. …LXXII. Conceder-se-á habeas data para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, considerado como um writ, uma garantia, um remédio constitucional à disposição dos cidadãos para que possam implementar direitos subjetivos que estão sendo obstaculados. 8. As informações fiscais conexas ao próprio contribuinte, se forem sigilosas, não importa em que grau, devem ser protegidas da sociedade em geral, segundo os termos da lei ou da constituição, mas não de quem a elas se referem, por força da consagração do direito à informação do art. 5º, inciso XXXIII, da Carta Magna, que traz como única ressalva o sigilo imprescindível à segurança da sociedade e do Estado, o que não se aplica no caso sub examine, verbis: Art. 5º.…XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. 9. In casu, o recorrente requereu à Secretaria da Receita Federal do Brasil os extratos atinentes às anotações constantes do Sistema de Conta-Corrente de Pessoa Jurídica-SINCOR, o Sistema Conta-Corrente de Pessoa Jurídica-CONTACORPJ, como de quaisquer dos sistemas informatizados de apoio à arrecadação federal, no que tange aos pagamentos de tributos federais, informações que não estão acobertadas pelo sigilo legal ou constitucional, posto que requerida pelo próprio contribuinte, sobre dados próprios. 10. Ex positis, DOU PROVIMENTO ao recursoextraordinário. (RE 673707, Relator(a): Min. LUIZ FUX, Tribunal Pleno, julgado em 17/06/2015, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO DJe-195 DIVULG 29-09-2015 PUBLIC 30-09-2015)

No STJ temos a mesma linha de pensamento, agora aplicada a normas infraconstitucionais que tratam do Direito do Consumidor e Sigilo Bancário[11]:

> EMBARGOS DE DECLARAÇÃO. RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. BANCOS DE DADOS. PROTEÇÃO AO CRÉDITO. PRIVACIDADE E

[11] STJ: RHC 78.162/RJ, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 27/11/2018, DJe 10/12/2018

INTIMIDADE. AUTODETERMINAÇÃO INFORMATIVA. DIREITOS FUNDAMENTAIS. EFICÁCIA HORIZONTAL. PRINCÍPIO DA MÁXIMA EFETIVIDADE. OBRIGAÇÃO DE NÃO FAZER.
ANOTAÇÕES. CARTÓRIOS DE PROTESTO. TERMO INICIAL DO PRAZO. ART. 43, § 1º, DO CDC. DATA DO VENCIMENTO DA DÍVIDA. MODULAÇÃO DOS EFEITOS. ART. 927, § 3º, DO CPC/15. PRINCÍPIO. PROTEÇÃO DA CONFIANÇA LEGÍTIMA. REGIME DE TRANSIÇÃO. ART. 23 DA LINDB. ÔNUS E PREJUÍZOS ANORMAIS OU EXCESSIVOS.
1 O propósito dos presentes embargos de declaração é determinar se são necessárias a modulação dos efeitos da condenação contida no acórdão embargado e a adoção de regime de transição para que a embargante se adeque ao comando contido em seu dispositivo (arts. 927, § 3º, do CPC/15 e 23 da LINDB).
2. A modulação de efeitos de decisão que supera orientação jurisprudencial é matéria apreciável de ofício, razão pela qual não configura inovação recursal.
3. O dever dos Tribunais de manter sua jurisprudência estável, íntegra e coerente cumpre o propósito de garantir a isonomia de ordem material e a proteção da confiança e da expectativa legítima do jurisdicionado, fornecendo-lhe um modelo seguro de conduta de modo a tornar previsíveis as consequências de seus atos.
4. A força vinculante do precedente, em sentido estrito, bem como da jurisprudência, em sentido substancial, decorre de sua capacidade de servir de diretriz para o julgamento posterior em casos análogos e de, assim, criar nos jurisdicionados a legítima expectativa de que serão seguidos pelo próprio órgão julgador e órgãos hierarquicamente inferiores e, como consequência, sugerir para o cidadão um padrão de conduta a ser seguido com estabilidade.
5. A modulação de efeitos do art. 927, § 3º, do CPC/15 deve ser utilizada com parcimônia, de forma excepcional e em hipóteses específicas, em que o entendimento superado tiver sido efetivamente capaz de gerar uma expectativa legítima de atuação nos jurisdicionados e, ainda, o exigir o interesse social envolvido.
6. O regime de transição do art. 23 da LINDB está em íntima conexão com o princípio da menor onerosidade da regularização, previsto no art. 21, parágrafo único, de referido diploma legal, segundo o qual não se pode impor aos sujeitos atingidos pela modificação de jurisprudência ônus ou perdas anormais ou excessivos.
7. Os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais.
8. In casu, ao menos desde o julgamento pela 3ª Turma do REsp 1316117/SC, ocorrido em 26/04/2016, não há jurisprudência consolidada em relação ao termo inicial do prazo máximo de inscrição da anotação nos cadastros de proteção ao crédito, o que permite concluir pela inexistência de jurisprudência em sentido substancial, capaz de ensejar nos jurisdicionados uma confiança racionalmente aceitável de estabilidade capaz de subsidiar uma legítima expectativa de certeza objetiva de resposta jurisdicional.
9. Ademais, não existe desproporcionalidade na imediata adoção da vedação ao registro de anotações negativas sem que conste a data de vencimento da dívida, pois a mera suspensão, até efetiva regularização do procedimento, da anotação de registros provenientes de cartórios de protesto que não contenham essa informação, não gera ônus excessivos ou desproporcionais para a embargante e evita a perpetuação dessa lesão aos direitos dos consumidores.
10. Embargos de declaração acolhidos sem efeitos infringentes.
(EDcl no REsp 1630659/DF, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 27/11/2018, DJe 06/12/2018)

Dessa forma, percebe-se que os nossos tribunais superiores já adotavam, na esfera constitucional e infraconstitucional a proteção de dados, porém em áreas do Direito que não diziam respeito e especificamente aos dados de saúde do indivíduo, o que se passou a partir do ano de 2018 ser disciplinado pelo CFM a partir da interpretação da Lei 13.709, por meio da Resolução CFM 2.227/2018.

Um dos casos mais emblemáticos e amplamente conhecido acerca do vazamento de dados médicos de paciente por profissional da saúde se deu no âmbito do aplicativo *Whattsapp*, quando a reumatologista do Hospital Sírio Libanês publicou, a um grupo de amigos do aludido aplicativo, informações sobre o estado de saúde da ex-primeira dama Maria Leticia Lula da Silva, mediante postagem de imagem de exame. Tal fato lhe rendeu a demissão do hospital Sírio Libanês, bem como uma sindicância no Conselho Regional de Medicina de São Paulo – CREMESP[12][13].

5.Conclusão

A revolução digital nos serviços de saúde veio disponibilizar novas oportunidades para o desenvolvimento da qualidade de prestação de cuidados de novos tratamentos e uma melhor utilização dos recursos. No entanto, em vários países o sistema de saúde está fortemente pressionado por vários fatores (gestão pública e privada, orçamentos, planejamento, priorização, interesses etc.).

A maioria das informações que, no atual cenário, é compartilhada pela via digital, anteriormente era feito pela via do papel, suscitando assim novos desafios e ameaças digitais ao nível da segurança e privacidade, nomeadamente em relação à proteção dos dados pessoais numa sociedade cada vez mais digital.

Verificou-se que existem legislações a nível estrangeiro (Argentina, Chile, Espanha, Portugal, Uruguai etc.) e nacional acerca da temática, e mais, a participação ativa do Conselho Federal de Medicina – CFM , bem como dos conselhos estaduais no combate e repressão aos vazamentos e abusos cometidos pelo uso indevido das informações médicas de pacientes.

No mesmo sentido nossos tribunais (STJ e STF) caminham alinhados no sentido de punir os agentes que violam a proteção de dados e fazem uso indevido das informações dos pacientes, clientes bancários, consumidores etc.

Verificou-se ainda que, existem casos reais de compartilhamento irregular de informações médicas de pacientes que detém um destacado *status* social, seja pela situação de ocupação de cargo político, artístico, familiares etc.

Além da curiosidade midiática, aponta-se o interesse comercial por empresas farmacêuticas e outras, bem como planos de saúde, na obtenção das informações médicas dos pacientes, as quais estão nos bancos de dados, para fins de montagem de uma estratégia de tratamento do indivíduo no cerne da empresa e condicionantes para a liberação de medicamentos ou procedimentos médicos a esses clientes.

Portanto, verifica-se que a questão é complexa diante da disputa de interesses por diversos agentes: empresas seguradoras e farmacêuticas, planos de saúde, pacientes etc., regulamentado com a intervenção do Estado por meio de suas legislações e decisões de seus tribunais, bem como os órgãos de classe (CFM e Conselhos Estaduais de Medicina) que visam a proteção da parte vulnerável nessa disputa, que é o cliente/paciente e seu histórico médico, que pelo visto aponta para uma consolidação protecionista a controlar as informações sensíveis no âmbito da atuação da Telemedicina, que desponta como uma inovação que visa estreitar laços e distâncias, entre o médico e o paciente, melhorando a atenção â saúde e a qualidade de vida.

Assim, o presente trabalho teve como objetivo trazer uma visão multifacetária, em diversos cenários de discussão (patentes, legal, jurisprudencial, midiático e doutrinária) quanto a importância e necessidade de proteção de dados, em especial, no âmbito da telemedicina (dados sensíveis), visando apresentar de forma completa como se encontra o estado da questão (problemática) no âmbito de alguns países do Mercosul e em Portugal.

[12] https://gauchazh.clicrbs.com.br/geral/noticia/2017/02/dados-vazados-sobre-estado-de-saude-de-marisa-leticia-abrem-debate-sobre-etica-medica-9713064.html. Acessado em 22.06.2019.

[13] https://jus.com.br/artigos/55669/sigilo-profissional-medico. Acessado em 22.06.2019.

Referências

AFONSO DA SILVA, VIRGILIO; Direitos fundamentais. Conteúdo essencial, restrições e eficácia. São Paulo: Ed. Malheiros, 2009. 279.

ARGENTINA. Ley 25.326. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acesso em: 21.06.2019.

BUENO, LUCIANO CORREIA BUENO.Sigilo profissional médico. O que o caso Marisa Letícia pode ensinar? Revista JUS. Disponível em: https://jus.com.br/artigos/55669/sigilo-profissional-medico. Acesso em: 21.06.2019.

BRASIL. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 21.06.2019.

BRASIL. Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21.06.2019.

BRASIL. Lei 12.414. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 21.06.2019.

BRASIL. Lei 12.527. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 21.06.2019.

BRASIL. Lei 12.965. Disponível em; http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21.06.2019.

BRASIL. Superior Tribunal de Justiça. Disponível em: http://www.stj.jus.br/sites/STJ. Acesso em: 21.06.2019.

BRASIL. Supremo Tribunal Federal. Disponível em: http://portal.stf.jus.br/. Acesso em: 21.06.2019.

CHILE. Ley 19.628. Disponível em: https://www.leychile.cl/Navegar?idNorma=141599. Acesso em: 21.06.2019.

Conselho Federal de Medicina. Disponível em: http://portal.cfm.org.br/. Acesso em 21.06.2019.

ESPACENET. Disponível em: https://worldwide.espacenet.com/. Acesso em: 21.06.2019.

FEIGELSON, BRUNO; ALBANI SIQUEIRA, ANTÔNIO HENRIQUE; Comentários à lei geral de proteção de dados.São Paulo: Ed. RT, 2019. 260.

INPI. Disponível em: http://www.inpi.gov.br/. Acesso em: 21.06.2019.

MENDES, LAURA SCHERTEL; Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Ed. Saraiva, 2014. 249.

MALDONADO, VIVIANE NÓBREGA; BLUM, RENATO OPICE; Lei Geral de proteção de dados comentada. São Paulo: Ed. RT, 2019. 250.

MALDONADO, JOSÉ MANUEL DE VARGAS. Telemedicina: Desafios à sua difusão no Brasil. Cadernos de Saúde Pública, Rio de Janeiro, 32,2, S1-S12, 2016.

ORBIT Intelligence. Disponível em: https://www.orbit.com/. Acesso em: 21.06.2019.

PORTUGAL. Regulamento 2016/679. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 21.06.2019.

SARLET, INGO WOLFGANG; MARINONI, LUIZ GUILHERME; MITIDIERO, DANIEL; Curso de direito constitucional. São Paulo: Ed. Saraiva, 2016. 1440.

SCHWAB, KLAUS. A quarta revolução industrial. São Paulo: Ed. Edipro, 2016. 159.

URUGUAI. Ley 18.331. Disponível em: https://www.impo.com.uy/bases/leyes/18331-2008. Acesso em: 21.06.2019.

Zero Hora. Disponível em: https://gauchazh.clicrbs.com.br/geral/noticia/2017/02/dados-vazados-sobre-estado-de-saude-de-marisa-leticia-abrem-debate-sobre-etica-medica-9713064.html. Acesso em: 21.06.2019.