E-SAUDE E OS DESAFIOS À PROTEÇÃO DA PRIVACIDADE NO BRASIL: UMA ANÁLISE DA GESTÃO DE DADOS PESSOAIS DE PACIENTES NO ÂMBITO DA LEI Nº 13.709/2018

Diego Costa Barbosa Santos[1]
Gabriel Aparecido Salvador de Moura[2]
Jordão Horácio da Silva Lima[3]

RESUMO

A evolução tecnológica tem impactado significativamente a área da saúde, especialmente através da e-Saúde, que engloba o uso de tecnologias de informação e comunicação na prestação de serviços de saúde. Este artigo analisa os desafios da proteção da privacidade na e-Saúde no Brasil, focando na gestão de dados pessoais de pacientes à luz da LGPD. A e-Saúde inclui prontuários eletrônicos, telemedicina, aplicativos móveis de saúde e dispositivos vestíveis, cada um com implicações distintas para a coleta e uso de dados pessoais. Os desafios incluem a necessidade de uma cultura de privacidade, capacitação contínua de profissionais e adequação das infraestruturas tecnológicas. Este estudo utiliza uma metodologia exploratória e revisão bibliográfica para analisar as nuances do direito à saúde e à privacidade, oferecendo uma análise crítica sobre a gestão de dados na e-Saúde e estratégias para superar os obstáculos na implementação de um ambiente digital seguro.

Palavras-chave: e-Saúde. Lei Geral de Proteção de Dados (LGPD). Segurança de dados. Privacidade.

1 INTRODUÇÃO

A evolução tecnológica tem transformado diversas áreas do conhecimento, e a saúde não é uma exceção. O advento da e-Saúde, que compreende o uso de tecnologias de informação e comunicação (TICs) na prestação de serviços de saúde, público e privado, tem promovido uma revolução na forma como os dados de pacientes são coletados, armazenados, compartilhados e utilizados.

Esta transformação, embora traga inegáveis benefícios, também levanta importantes questões relacionadas à proteção da privacidade e à segurança dos dados pessoais dos pacientes.

No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, surgiu como um marco regulatório essencial para abordar essas questões. Estabelecendo

[1] Acadêmico, Faculdade Evangélica Raízes, Anápolis, Goiás, diego_18go@hotmail.com.
[2] Acadêmico, Faculdade Evangélica Raízes, Anápolis, Goiás, gabriel.apsmoura@gmail.com.
[3] Doutor em Saúde Global e Sustentabilidade (USP); Mestre em Saúde Global e Diplomacia da Saúde (Fiocruz), advogado, professor titular, Faculdade Evangélica Raízes, Anápolis, Goiás, e-mail.

diretrizes sobre o tratamento de dados pessoais, buscando assegurar o direito à privacidade e à proteção dos dados pessoais dos indivíduos e, no contexto da e-Saúde, a implementação desta lei apresenta desafios específicos, dada a natureza sensível das informações envolvidas.

Este trabalho tem como objetivo analisar os desafios à proteção da privacidade no âmbito da e-Saúde no Brasil, com um foco particular na gestão de dados pessoais de pacientes à luz da LGPD.

A contextualização do tema passa pelo entendimento da e-Saúde como um conceito abrangente, que inclui desde prontuários eletrônicos e telemedicina até aplicativos móveis de saúde e dispositivos vestíveis. Cada uma dessas tecnologias possui diferentes implicações para a coleta e o uso de dados pessoais, aumentando a complexidade da gestão dessas informações. Além disso, a globalização e a digitalização crescente dos serviços de saúde ampliam a necessidade de um marco regulatório robusto e eficaz.

A relevância da privacidade dos dados de saúde é, além de um direito inerente ao humano, inquestionável. Dados de saúde são considerados dados sensíveis pela LGPD, pois envolvem informações íntimas e confidenciais sobre a condição física e mental dos indivíduos.

A divulgação não autorizada ou o uso inadequado desses dados pode resultar em discriminação, estigmatização e outros impactos negativos significativos para os pacientes, muitos ainda nem imaginados.

A LGPD, introduz princípios e obrigações que visam garantir a transparência, segurança e controle dos dados pelos titulares. No que tange a e-Saúde, a aplicação da LGPD exige uma adaptação rigorosa por parte dos profissionais de saúde, instituições e desenvolvedores de tecnologia. A gestão de consentimentos, a implementação de medidas de segurança adequadas e a garantia de direitos dos titulares são apenas alguns dos aspectos críticos a serem considerados.

Por sua vez, os desafios na implementação da LGPD na e-Saúde no Brasil são diversos. Entre eles, destaca-se a necessidade de uma cultura de privacidade e proteção de dados nas instituições de saúde, a capacitação contínua de profissionais para lidar com questões de segurança da informação, e a adequação das infraestruturas tecnológicas às exigências legais.

Adicionalmente, a interoperabilidade dos sistemas de saúde e a conformidade com a legislação são questões complexas que demandam soluções inovadoras e um comprometimento sério de todas as partes envolvidas.

Diante desse cenário, este estudo busca aprofundar a compreensão dos desafios à proteção da privacidade na e-Saúde, oferecendo uma análise crítica sobre a gestão de dados pessoais de pacientes no Brasil.

Ao longo do trabalho, serão exploradas as implicações da LGPD para o setor de saúde, as melhores práticas de gestão de dados, e as estratégias para superar os obstáculos encontrados na implementação de um ambiente digital seguro e respeitoso à privacidade dos pacientes.

Para tanto, a pesquisa baseou-se no método exploratório e em uma revisão bibliográfica de artigos concernentes à proteção de dados pessoais, e regulamentação referente à tecnologias sanitárias relacionadas com a e-saúde, visando a elucidação do fenômeno proposto, aplicando-se a pesquisa qualitativa e objetivando uma análise das nuances do direito constitucional à saúde e à intimidade, partindo-se da premissa bibliográfica indicativa, no intuito de estreitar os limites do objeto central proposto.

2 ENTENDIMENTO HISTÓRICO-SOCIAL

O constante avanço das tecnologias da informação e, por decorrência, da comunicação tem transformado a forma como as pessoas interagem com o mundo ao seu redor em todos os âmbitos sociais, inclusive na forma em que a saúde é acessada e, de certo modo, consumida.

Em um ambiente de constante transição técnica, migrando os meios e mecanismos analógicos e materiais para planos digitais e eletrônicos, o acesso a saúde passou a se desenvolver, em muitas frentes, de modo híbrido, com sua principal fonte sendo democratizada por mecanismos digitais e seus pilares sociais fixos ao meio analógico.

Nesse contexto, a *e-saúde*, nomenclatura que vem se consolidando com o passar dos anos, foi ilustremente definida, sobretudo aos padrões da época, de forma breve, como o uso das TICs (tecnologias da informação e comunicação) para melhorar a qualidade, a eficiência e a acessibilidade dos diferentes povos aos serviços de saúde em diferentes níveis, pelo professor Vincenzo Della Mea (2001), no artigo

“*What tis e-health: the death of telemedicine?*” publicado online pelo National Library of Medicine.

Fato é que o ato de incorporar mecanismos tecnológicos, mesmo que oriundos de outras searas do conhecimento, para o aprimoramento da forma em que parcelas cada vez maiores da população possuem de acessar a saúde, pública ou privada, direito uno a si, trazem diversos benefícios inerentes a sua implementação, ao passo em que desbravam desafios de teor logístico, comunicativo, tecnológico e legal.

Mesmo que parcelas sub atendidas, ou de difícil acesso aos meios tradicionais de saúde, seja medicamentoso ou hospitalar, possam ter um novo e mais expansivo meio de acesso a um direito humanitário básico, estados-nação, pela via estatal, já começam a sentir os impactos desse tipo de implementação.

Ao mesmo tempo em que famílias residentes em regiões, quase, inacessíveis passam a ter o mínimo de atendimento por meio da telemedicina, por exemplo, o seu acesso a medicamentos e especialistas humanos se mantém tão ruim quanto jamais foram e, a depender do momento, se tornam ainda piores. Com toda melhoria significativamente avançada, os agentes responsáveis pelo aprimoramento das políticas públicas se acomodam ainda mais no pouco desenvolvimento que tiveram, sucateando e segregando setores que, de modo geral, já são, e estão, sucateados mesmo em tempos onde tais tecnologias sequer eram projetadas.

Ao contrário do que se possa imaginar, o problema real por trás do desabastecimento, ou do escárnio e estigma ligado a saúde a famílias sub atendidas, é a logística, não a sua implementação, mas a prioridade no qual ela possui.

A CRFB - Constituição da República Federativa do Brasil, promulgada em 1988, torna claro, durante todo o Título II, dedicado aos Direitos e Garantias Fundamentais, em seu artigo 6º, o pleno direito a todos os cidadãos à saúde nos seguintes moldes:

> Art. 6º. São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição (Brasil, 1988).

No entanto, mesmo restando claro que o direito a saúde é um dos inúmeros direitos e garantias fundamentais e inerentes a todo ser humano, e sendo praste que a CRFB/88 nivela todo o povo brasileiro ao mesmo patamar de igualdade de direitos

e obrigações, nos termos do art. 5º, inciso I, os próprios entes públicos, dotados da máquina pública, imbuídos de boa-fé e responsáveis por fazer tais entendimentos se valerem a realidade, por vezes, se ausentam de suas obrigações e escanteiam o atendimento devido e pleno à povos historicamente marginalizados.

Ad exemplum, a saúde pública para povos marginalizados, como os indígenas, tem enfrentado desafios significativos no Brasil. De acordo com uma reportagem da Deutsche Welle – DW (Modelli, 2023), apenas 180 médicos estão trabalhando em distritos específicos para indígenas em todo o país. Sendo que, mesmo nessas poucas instalações de trabalho, as condições e instalações precárias são o maior obstáculo para os agentes de saúde realizarem os seus serviços de modo adequado.

Fatos estes, destacados de modo brilhante no artigo “Desigualdades de gênero e raciais no acesso e uso dos serviços de atenção primária à saúde no Brasil” (Cruz, 2021), que evidenciam o principal fator para uma disparidade do modo de acesso e atendimento à saúde por povos de diferentes classes sociais, o mero interesse.

> No Brasil, o advento da pandemia em março de 2020 encontrou um sistema público de saúde universal em direitos no que concerne ao acesso a seus serviços, porém com graves distorções e gargalos de atendimento, em especial àqueles referentes à atenção primária de saúde, porta de entrada do Sistema Único de Saúde (SUS). Pontos nevrálgicos históricos do atendimento público hospitalar foram ainda mais expostos, como o Sistema de Regulação (SISREG) responsável pelas conhecidas filas de espera por consultas, exames e cirurgias; a lotação ou ausência de leitos hospitalares; a desigual distribuição de recursos e equipamentos e a clivagem público-privada no acesso à saúde (Cruz, 2021, p. 4022).

Por outro lado, não há que se falar em ponto focal, mesmo que o fator logístico tenha seu grau de importância, a falta de comunicação clara e precisa, oriunda de uma rede organizada em prol deste bem, também influenciam nas relações sociais frente ao acesso à saúde e a informação.

Como dito na reportagem do Nexo Políticas Públicas (Thami, 2021), intitulada de “6 pontos sobre a relação entre comunicação e saúde”, durante a pandemia, o Brasil demonstrou não só a falta de planejamento de campanhas coordenadas de comunicação em saúde, mas também um forte conflito de mensagens e até mesmo propagação de informações incontestavelmente falsas ou sem qualquer com pouco embasamento científico.

Isso é particularmente problemático no contexto da e-saúde, onde a comunicação eficaz é essencial para garantir que os pacientes recebam informações precisas e atualizadas sobre seu estado de saúde.

Ademais, os avanços tecnológicos constantes e frenéticos também podem trazer desafios significativos para a e-saúde. De acordo com uma reportagem do portal ShareCare (2022), um dos principais problemas é o aumento da distração causada pelo uso excessivo da tecnologia. De acordo com a matéria, com mais facilidade de acesso à internet, as pessoas podem ter contato com uma maior quantidade de informações, o que aumentaria o nível de distração, dentro e fora dos ambientes hospitalares.

Outro desafio ligado aos avanços tecnológicos inerentes a área é a proteção de dados sigilosos destes ambientes, no qual hackers e outros criminosos poderiam acessar dados médicos privativos de algum paciente. Fator particularmente problemático no contexto da e-saúde, onde a segurança dos dados do paciente são, e devem, ser tratados como de extrema importância.

Por fim, a falta de legislação inerente a matéria, sendo brevemente desenvolvida em legislações como nas Leis nº 12.965/2014 e 13.709/2018, respectivamente nomeadas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD), estabelecem um terreno subjetivo e turvo de atuação do setor privado que, ao passo em que seguem o pouco que há rente à matéria, estabelece meios, preceitos e temas discutíveis neste âmbito, algo que se desenvolve em paralelo em diferentes pontos do globo terrestre.

2.1 PROBLEMÁTICA SISTÊMICA DE UM MEIO DIGITALMENTE DEPENDENTE

Cabe relembrar que a e-saúde é um campo emergente na intersecção de tecnologia da informação, negócios e saúde em diferentes pontos do mundo, interconectados por ambientes digitais e globalizados em constante expansão.

No entanto, a implementação da e-saúde enfrenta vários desafios a nível nacional e internacional, sendo um deles, a proteção da privacidade e a gestão de dados pessoais de pacientes.

A Lei nº 13.709/2018 do Brasil, também conhecida como Lei Geral de Proteção de Dados (Brasil, 2018), estabelece diretrizes claras sobre como os dados pessoais devem ser gerenciados no contexto da saúde.

> Art. 5º. II. dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018).

Como bem observado por Tania Aparecida Soares (2022), no artigo “Os Impactos da Lei Geral de Proteção de Dados – LGPD no Cenário Digital”, o artigo 11 da LGPD se aplica ao tratamento de dados pessoais sensíveis, dispostos de modo claro no artigo supracitado (art. 5º, inciso II), resguardando, acima de tudo, a revelação de dados que possam causar prejuízos ao titular, caso venha a ser compartilhado entre os controladores, visando vantagem econômica ao agente causador ou a terceiro que possa, de algum modo, estar envolvido.

Ainda segundo ao artigo, a violação desta norma pode acarretar, inclusive, sansões do poder público, em suas diferentes áreas de atuação e competências.

No entanto, mesmo que este tipo de normativa e penalização seja aplicado de modo feroz, eficiente e utópico, o cenário possível onde dados sensíveis ligados a saúde de determinada população está, ou pode estar, sendo vazada a fim de beneficiar redes privadas, como seguradoras ou hospitais, já encobrem todo o cenário por uma nevoa de dúvida que me é, sem margem a dúvida, calamitoso.

O jogo eletrônico estadunidense *Watch Dogs 2* (2016), publicado pela Ubisoft Montreal, evidencia de modo alarmante e exagerado o impacto que uma rede globalizada e puramente virtual causa na vida da população de modo geral.

Mesmo se tratando de uma obra ficcional, o jogo eletrônico satiriza e extrapola a problemática de empresas conseguirem acesso a dados considerados sensíveis, também, pela legislação brasileira.

Em determinada *quest*, o jogo evidencia apenas um efeito nefasto, ao protagonista se deparar com uma rede de dados confidenciais perdendo seu escopo sigiloso a benefício de corporações privadas, no caso, empresas de seguro modulando em tempo real o valor do seguro de vida de toda uma família com base

em um conjunto de dados coletados desde a infância por dispositivos como *smartphones* e até geladeiras.

Notório que o jogo, por se tratar de uma obra de ficção, idealiza um cenário a fim de causar choque e comoção. Mas ver um exemplo claro e, de certo modo, cada vez mais próximo, de como esses dados podem estar sendo utilizados para fins, mesmo que em grau reduzido, verossimilhante, já é preocupante o suficiente.

De todo modo, a preocupação não reside apenas em obras ficcionais de entretenimento, Suely Deslandes e Tiago Coutinho (2022), ao observarem as relações sociais em ambientes digitais, sobretudo em período da pandemia de COVID-19, provocado pelo vírus *SARS-CoV-2*, por meio do artigo “Pesquisa social em ambientes digitais em tempos de COVID-19: notas teórico-metodológicas” discorrem o seguinte:

> Os desenvolvimentos e desafios atuais em uma perspectiva internacional e suas reverberações no contexto nacional sugerem que pode estar chegando a hora de mudança do “paradigma” da ATS enquanto campo científico, no sentido Kuhniano. As bases teóricas e metodológicas que orientaram a seleção, a avaliação e a crítica dos critérios relevantes a serem verificados nesses estudos devem ser revistas para se adequarem às novas demandas da sociedade. A aproximação interdisciplinar com outros campos de conhecimento (Filosofia, História, Política, Sociologia, Antropologia e Direito) poderá fortalecer sua fundamentação teórica e potencializar seu uso e, dependendo da intensidade de todas essas mudanças, elas poderão gerar uma revolução nesse campo científico. Essa dinâmica dependerá amplamente da formação de mecanismos de ação política e sociais negociados também pela comunidade de pesquisa. As mudanças paradigmáticas dependerão fortemente, portanto, de elementos exteriores à ciência (Coutinho, 2022).

Importante ressaltar, por fim, que o cenário plausível, proveniente de um avanço exacerbado das tecnologias da informação e comunicação, a primeiro olhar, se mostram otimistas e frutíferos, cedendo, porém, as impurezas da natureza humana, desvirtuando o seu suposto significado e objetivo natural, pressupondo, é claro, que algo de magnitude suficientemente capaz de reverberar e modular por completo todo o paradigma social e cultural de toda a civilização humana possua um objetivo ou significado natural, tampouco que este seja benefício à espécie humana.

Diferente do que pressupor algo sobre uma tecnologia em acessão, é necessário olhar além do que sua própria existência, se atendo, sobretudo, aos seus efeitos práticos no avanço de todo um contingente social, a *priori*, modular e consistente, mas que encara, em última análise, dificuldades e barreiras inerentes a algo inédito, afinal, é disso que se trata, de um avanço inédito em uma área pouco

conhecida que, inevitavelmente, modifica por completo toda e qualquer forma de desenvolvimento social.

3 RISCOS COMPORTAMENTAIS

A ancoragem mítica por trás dos efeitos danosos provindos do constante avanço tecnológico, embora alarmantes e espalhafatosos, resvalam em um teor verossímil quando aplicado a materialidade fática, anteriormente restrita à pequenos grupos de interesse que, aos poucos, se mostram também ao grande público.

Em março de 2023, Shou Zi Chew, o CEO global do *Tik Tok,* notória empresa de mídia social e entretenimento, fora convocado pelo Congresso estadunidense para prestar esclarecimentos sobre a influência fática que seu produto, a mídia social, exerce sobre a mentalidade humana, sobretudo aos jovens e adolescentes (Thorbecke, 2023).

Questões irrisórias e banais foram levantadas por parlamentares do que é, provavelmente, o congresso mais poderoso e influente de todo o ocidente, o que não muda o fato de que as preocupações são válidas e legitimas.

De acordo com Catherine Thorbecke (2023), repórter da CNN, um deputado de Nova Jersey destacou uma pesquisa estadunidense descobriu que “os algoritmos do TikTok recomendam vídeos para adolescentes que criam e exacerbam sentimentos de sofrimento emocional, incluindo vídeos que promovem suicídio, automutilação e transtornos alimentares”, embora não evidenciando a fonte exata para a informção.

Outro deputado, agora representativo do Estado de Ohio, havia acusado, a mesma sessão, que o *Tik Tok* estaria promovendo conteudos do chamado “*desafio do blecaute*” para crianças de e adolescentes, resultando, teoricamente, na morte de uma criança de 10 anos do Estado da Pensilvânia.

Ainda nesta audiência, o deputado Gus Bilirakis, eleito pela Flórida, ressaltou uma série de preocupações quanto à tecnologia e o algoritimo por trás da mídia social que estaria, teoricamente, abrindo espaço para que crianças sejam expostas a conteúdos nocivos, resutando na emblemática frase “*Sua tecnologia está literalmente levando à morte*”.

Talvez não por coincidência, poucos meses após esta audiência, tendo o *Tik Tok* como principal alvo, aplicou uma série de atualizações de segurança, alterou seus

termos de uso e implementou uma série de recursos a fim de exercer uma proteção adicional para os usuários “mais jovens”. Vale-se dizer que o movimento fora replicado pelas demais *big techs* do setor.

Fato inegável que o hiperestimulo gerado pelo constante uso de dispositivos eletrônicos vem ocasionando em um aumento vertiginoso em patologias psiquiatricas como a depressão, trastornos do humor, bipolaridade, transtornos de ansiedade e, principalmente, Transtorno de Defict de Atenção e Hiperatividade - *TDAH* (Nabuco, 2008).

Deve-se ater, ainda, que mesmo que estas patologias possam estar sendo mais bem relatadas e expostas como pertencentes às novas gerações, atribuindo um carater de epidemia geracional, generalista por óbivio, o estudo “Dependência de Internet e de Jogos Eletrônicos: uma revisão”, públicado em 2008, evidência que tal infleuncia não se restringe a faixas etárias ou a cultura preexistentes:

> A Dependência de Internet pode ser encontrada em qualquer faixa etária, nível educacional e estrato sócio-econômico. Inicialmente, acreditava-se que esse problema era privilégio de estudantes universitários que, buscando executar suas atribuições acadêmicas, acabavam por permanecer mais tempo do que o esperado, ficando enredados na vida virtual. Entretanto, tais pressuposições mostraram ser pura especulação. Sabe-se, hoje, que à medida que as tecnologias invadem progressivamente as rotinas de vida, o contato com o computador cada vez mais deixa de ser um fato ocasional e, portanto, o número de atividades mediadas pela Internet aumenta de maneira significativa, bem como o número de acessos e tempo medido na população brasileira que, atualmente, ocupa o primeiro lugar no mundo em termos de conexão doméstica (Abreu, 2008, p. 4)

Tal fato se reafirma quando observamos que a empresa Cambridge Analytica utilizou, ilegalmente, dados de mais de 87 milhões de usuários fornecidos pelo Facebook, hoje pertencente ao grupo *META*, para influenciar multidões e manipular artificialmente o resultado das eleições presidenciais e estaduais dos EUA no ano de 2016. Fato descoberto somente em 2018 e reportado em todos os jornais, editoriais e portais jornalísticos independentes nas mesmas mídias sociais que trouxeram todo este escândalo à tona.

Ao ver um contingente significativo de pessoas votantes, em sua maioria com vida estável, família constituída e um nível satisfatório de escolaridade, se torna inviável defender que apenas as novas gerações estariam sendo influenciada por todos esses algoritmos e redes digitais.

A realidade se impõe.

Mesmo que um grande contingente tenha sido influenciado politicamente, fato relativamente isolado, não é possível auferir que as mídias sociais são utilizadas como mecanismos de manipulação emocional, correto?

Errado.

Um estudo realizado por Andrew G. Reece e Christopher M. Danforth (2017), publicado pela *EPG Data Sciencie*, intitulado "*Instagram photos reveal predictive markers of depression*" revelou que apenas a análise previa de postagens públicas nos perfis dos usuários do *Instagram* já é o suficiente para traçar marcadores confiáveis de pacientes com depressão.

O estudo focou na análise e monitoramento continuo de 166 usuários, nos quais 71 (42%) já foram diagnosticas por depressão, a partir de suas postagens públicas em seu *feed* e *stories* e, a partir daí, encontrar uma correlação entre aqueles que possuem diagnóstico positivo.

Aqueles usuários já diagnosticados possuíam postagens em tons frios de cor, com movimentações discretas e pouca incidência de terceiros em suas postagens.

O fato curioso é que, estendendo estes marcadores para uma amostra de 43.950 usuários do *instaram*, foi possível auferir com um percentual significativo de acertos não só aqueles que estavam já diagnosticados com a patologia, mas sim aqueles que viriam a receber tal diagnóstico ao decorrer do estudo. Conclusões extraídas apenas por dados públicos.

E o mesmo se mostrou verdade quando analisado usuários que eram expostos a padrões muito específicos de postagens gerando uma mudança espaçada e quase imperceptível na personalidade dos usuários que eram mostrados *posts* taxados como "tristes" ou "solitárias". A recíproca se mostrou verdadeira ao apresentar conteúdos taxados como "felizes" e "motivadores" a usuários com predisposição a depressão.

Muito além do que pensar em um possível tratamento alternativo a esta patologia, o que o estudo fez foi reafirmar algo que estava restrito apenas ao chamado senso comum.

As mídias sociais influenciam sim na personalidade e motivação de seus usuários. Mesmo que ambas as partes neguem tal alegação, a realidade se impõe.

3.1 RISCOS AO ARMAZENAMENTO

Do mesmo modo que as mídias sociais coletam dados extensivos dos usuários digitais, inclusive com potencial de venda, embora velada, das informações que seriam, primariamente, privadas, as grandes seguradoras e planos de saúde coletam e auferem seus dados “públicos” a fim de estipular uma faixa de cobrança, aceitar ou negar clientes, fornecer medicamentos e amparar enfermos conveniados.

Grandes redes de hospitais e farmácias realizam algo semelhante.

Ao passo em que possuem um sistema unificado de dados, permitindo que o mesmo cliente possa ir à dois hospitais da mesma empresa sem que realize dois cadastros prévios, por exemplo, ou que ele possa aproveitar de seu cupom no aplicativo da Drogaria X, pertencente a uma vasta rede de drogarias para adquirir medicamentos em qualquer loja desta rede em todo o pais, gerando um alto nível de comodidade e fluidez ao usuário, tais tecnologias coletam e armazenam informações de consumo e geolocalização a fim de identificar padrões de consumo e predeterminar possíveis ações futuras.

Sistemas de análise de crédito realizados por seguradoras no momento de aceitar ou não determinado paciente em sua cartela de clientes sofrem influencias dessa vasta rede unificada de dados.

Não seria apenas coincidência que marcas como a *Colflex, Dramin, Engov, Finn, Zero-cal, Neo Química, Tamarine, Vitasay, Benegrip, Addera*, dentre outras, além de investimentos no setor de fabricação de fraudas, escovas dentais, itens de higiene bucal e a empresa *My Agencia de Propaganda* são de propriedade da mesma empresa mãe, a *Hypera Pharma*. (Hypera Pharma, 2023).

Mesmo estando estipulado na LGPD (2018) que “a proteção de dados pessoais é um direito fundamental”, a mera existência de corporações com tamanha quantidade de dados privativos computados e armazenados já representa um risco suficiente grande à sociedade brasileira.

Em primeira tese, pressupor que tais dados coletados por entes privados, de pequeno, médio ou grande porte, esteja em total segurança se demonstra leviano por si só.

Dados pessoais coletados por diferentes dispositivos vinculados, ou não, aos grandes servidores podem ser, e são, no melhor dos cenários, utilizados para propagação de mídia e marketing.

3.2 IMPLICAÇÕES LEGAIS

Por meio da LGPD (2018), em seu artigo 1º, o Estado incumbiu a si o dever de resguardar os dados privativos do povo brasileiro, de modo que o mundo privado, e suas liberdades individuais, de cada cidadão seja preservado e desenvolvido.

> Art. 1º. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Tal incumbência se reafirma a medida em que a Emenda Constitucional 115, de 10 de fevereiro de 2022, adicionou à Carta Magna o reconhecimento da proteção de dados pessoais como um direito fundamental.

Isso significa, em última medida, que o Estado tem a responsabilidade autoimposta de garantir a privacidade e a segurança dos dados pessoais dos cidadãos. Além disso, a proteção dos dados pessoais também é garantida de forma indireta através da previsão da ação de habeas data (art. 5º, LXXII, da CF), que busca assegurar ao indivíduo o conhecimento e a possibilidade de buscar a retificação de dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público.

Como implicações claras, em sendo dever do Estado presar pelo sigilo pleno de dados privativos de seus cidadãos, podendo aplicar sansões administrativas, inclusive multas, para as chamadas *big techs*¸ empresas detentoras da maioria dos dados digitais dispostos na *internet*.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a

> sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); IX - (VETADO). X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (Brasil, 2018).

A proteção de dados privativos e sensíveis por parte do estado, como direito fundamental do povo brasileiro se estendeu, por consequência, ao Conselho Federal de Medicina (CFM), principal órgão regulador da atividade profissional ligado à saúde.

O princípio profissional do sigilo e da confidencialidade entre a relação médico x paciente, antes atrelado a meios analógicos, passou a vigorar também em relações digitais antes mesmo do advento do Marco Civil da Internet (2014) e da LGPD (2018).

O artigo 73 do Estatuto de Ética do Conselho Federal de Medicina (EECFM), no qual trata do segredo as informações obtidas no exercício da atividade profissional se comunica de modo impar aos artigos 11 da LGPD e 7º do Marco Civil da internet que dispõem, respectivamente, sobre a garantia da confidencialidade dos dados pessoais dos usuários e da inviabilidade da intimidade e da vida privada, mesmo em ambientes virtuais.

> Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente (EECFM, 2019, pg. 35).
>
> 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 (Brasil, 2018).
>
> 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 (Brasil, 2014).

A responsabilidade coletiva e social quanto a privacidade vem, sobretudo, para atender a princípios éticos e filosóficos que, de modo efetivo, interferem na relação de convívio entre os cidadãos de todas as nações.

No entanto, mesmo em se tratando de direito fundamental, pétreo a qualquer cidadão, estando sob o encargo do Estado, primariamente, o dever de proteger e manter o sigilo a privacidade dos dados digitais, sobretudo sanitários, se estendendo subsidiariamente ao setor privado o dever de preservar e manter sob sigilo os dados pessoais dos consumidores, o próprio Estado se encarrega de prover tais dados sobre o pretexto de “relevante interesse público.

É alçado ao relento direitos fundamentais e inerentes ao indivíduo a fim de justificar uma mera investigação policial, fato corrente é percebido de modo claro na decisão prolatada no Superior Tribunal de Justiça, no Recurso em Mandado de Segurança (RMS) 61.302-RJ, de relatoria do Ministro Rogério Schietti Cruz, no qual traçou novas diretrizes sobre a quebra de sigilo dos dados informáticos.

> 2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública (STJ. RMS 61.302-RJ. Rel. Min. Rogerio Schietti Cruz, Terceira Seção, por maioria, julgado em 26/08/2020, DJe 04/09/2020).

A eminente ementa reforça um fato de pela concordância entre os juristas, nenhum direito é absoluto. Ao ponto em que o direito a privacidade pessoal e, por consequência, aos dados informativos é de caráter pétreo e fundamental, há casos em exceção no qual o sigilo aos dados privativos é quebrado em prol do interesse público.

No caso em epigrafe, foram tratados de dados de geolocalização de registro geral que, de alguma forma, serviriam na identificação de suspeitos de um crime de homicídio.

Por mais que o objetivo fim seja nobre e, no caso fático supracitado de fato é, a ideia de turvar um direito fundamenta ao be prazer do Estado, preconizando “o interesse público” se torna um risco existencial ao próprio Estado democrático de direito e, por efeito lógico, à própria dinâmica social.

4 NOVAS DINÂMICAS SOCIAIS

O embate entre o avanço tecnológico, os meios digitais e a privacidade de dados médicos e sensíveis assume uma dimensão cada vez mais complexa e crucial no contexto contemporâneo.

No cerne dessa discussão está, sem dúvidas, o equilíbrio delicado entre o progresso tecnológico e a preservação da privacidade inerente ao usuário e dos direitos humanos fundamentais.

A crescente digitalização dos registros médicos e a coleta massiva de dados pessoais impõem desafios significativos para o arcabouço legal existente, prejudicado por uma defasagem grosseira e pouco atenta.

Embora legislações como a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, tenham sido promulgadas para estabelecer diretrizes claras sobre o tratamento de dados pessoais e sensíveis, sua implementação e aplicação efetiva ainda enfrentam obstáculos consideráveis.

É difícil precisar de forma objetiva as razões pelas quais o pouco já legislado vem sendo negligenciado nas mais diversas correntes sociais, inclusive do Direito.

Questões como a definição de padrões de segurança cibernética, a responsabilidade pelo vazamento de informações e os limites do consentimento do usuário, por meio dos chamados “termos de uso” continuam demandando atenção e aprimoramento.

Como já citado anteriormente, *“A Dependência de Internet pode ser encontrada em qualquer faixa etária, nível educacional e estrato sócio-econômico”* (CRISTIANO ABREU, 2008), tais características, em se tratando da volubilidade do extrato social no qual as redes virtuais se abrangem, impõem um risco social que, ao meu ver, é bastante negligenciado.

Além disso, aspectos éticos emergem no contexto da e-saúde, levantando questionamentos sobre a autonomia do paciente, a confidencialidade das informações médicas e o uso ético dos dados para pesquisa e desenvolvimento cientifico e cultural.

Embora imposto à toda classe médica brasileira, mediante o Estatuto de Ética Médica, é de notório saber que, independentemente do nível de vigilância e curadoria, se denota virtualmente impossível garantir pela proteção dos dados privativos de todos os pacientes de todos os profissionais da saúde.

A proteção da privacidade não deve ser apenas uma obrigação legal, abarcada como dever próprio do Extado, mas também um imperativo ético para todas as partes envolvidas.

O que, infelizmente, não pode ser garantido.

4.1 IMPACTOS CULTURAIS

O avanço das tecnologias digitais tem transformado profundamente a dinâmica social e cultural, influenciando não apenas a forma como interagimos, mas também nossa percepção de privacidade, segurança e liberdade, fato que se corrobora a medida em que os indivíduos recorrem cada vez mais às mídias digitais como meio formador de prova idônea para a solução de seus próprios conflitos.

Mas a cena muda quando tratamos da aplicabilidade de normas legais e soberanas de um Estado-Nação em um ambiente turvo e obscuro como as mídias digitais, por exemplo.

No artigo “A Regulação de Conteúdo nas Redes Sociais: uma breve análise corporativa entre o NetzDG e a solução brasileira” publicada em 2022 por Gabriel Brega, fica nítido que a solução brasileira, mediante Marco Civil da Internet (Lei nº 12.965/2014) e, posteriormente, a LGPD, se demonstra leviana e ultrapassada, não se aplicando a correntes e evoluções sociais dos últimos anos como se esperava que se aplicaria.

> Contudo, ao se analisar um sistema jurídico que adotou um regime de responsabilização distinto, mais severo, percebe-se que o resultado obtido não é satisfatório. Os provedores de redes sociais, ainda que ameaçados por multas milionárias, acabaram por remover mais aquilo que está em desacordo com sua política interna. Ainda que se imponha maior celeridade ao processo de análise, e que certos conteúdos que antes não seriam removidos passem a ser, as consequências negativas de tal disposição não compensam os parcos ganhos. A propósito, além dos riscos para a liberdade de expressão, há a alocação de um poder excessivo nas mãos dos provedores, que passam a exercer a função de interpretação da lei (e não somente de suas diretrizes internas), o que deveria ser feito somente pelo Poder Judiciário (Brega, 2022, p. 21)

A proliferação de mídias sociais, dispositivos conectados e aplicativos de saúde cria novas oportunidades de acesso à informação e serviços, mas também expõe os usuários a riscos de vigilância, manipulação e discriminação.

A noção de privacidade, antes associada principalmente ao espaço físico, agora é permeada pela esfera digital, onde nossas atividades online deixam rastros permanentes. Isso levanta questões sobre o controle e a propriedade dos dados pessoais, bem como sobre a transparência e a prestação de contas das entidades que os coletam e utilizam.

Em termos culturais, a crescente dependência de tecnologias digitais pode influenciar padrões de comportamento, percepções de identidade e até mesmo a saúde mental das pessoas.

O fenômeno do "vício em tela" e a pressão social exercida pelas mídias sociais por um padrão cada vez mais fantasioso destacam a necessidade de uma abordagem holística para lidar com os impactos psicossociais do mundo digital, muito além de meras implicações jurídicas que uma geração consolidada por mecanismos como "*deep fakes"* e Inteligências Artificiais.

4.2 E-SAÚDE E OS DESAFIOS DA POLITICA PÚBLICA E NA SAÚDE SUPLEMENTAR

A implementação da e-saúde, especialmente no contexto brasileiro, apresenta desafios significativos quando consideramos a complementaridade ou suplementaridade em relação às políticas públicas de saúde.

A e-saúde, que abrange a utilização de tecnologias da informação e comunicação (TIC) para melhorar os serviços de saúde, enfrenta obstáculos específicos quando integrada com a política pública suplementar, que se refere aos serviços de saúde oferecidos por empresas privadas de seguro saúde.

No Brasil, o sistema de saúde é marcado pela coexistência do Sistema Único de Saúde (SUS) e dos serviços privados de saúde. A e-saúde, como meio tecnológico e modalidade una a si, precisa lidar com essa fragmentação, garantindo interoperabilidade entre sistemas públicos e privados para fornecer uma experiência de saúde contínua e integrada para os pacientes, de modo uníssono a garantir a privacidade e segurança dos usuários.

> Um fator que talvez nos ajude a compreender a escassa entrada do campo de políticas públicas (ou *Policy Sciences*) no campo da saúde pública é o fato de que se trata, ao contrário do que ocorre com outras práticas disciplinares, de uma perspectiva analítica voltada para problemas sociais e políticos

> específicos, visando inclusive a intervenção, tornando a abordagem necessariamente multidisciplinar e explicitamente orientada por valores (Oliveira, 2016, p. 4).

A interoperabilidade entre sistemas de informação de saúde é essencial para garantir a eficiência e a qualidade do atendimento ao paciente.

A política púbica suplementar, modalidade popular por sua flexibilidade e preços competitivos, caracteriza-se pela divisão dos custos de planos de saúde entre empresas, empregados e aposentados. No entanto, essa modalidade apresenta particularidades na gestão de dados de saúde que exigem atenção redobrada à luz da LGPD.

Diferentes entidades, como empresas, operadoras e prestadores de serviços, manipulam os dados do paciente, aumentando o risco de violações e dificultando o controle do fluxo de informações.

A natureza da política cúbica exige o compartilhamento de dados entre os envolvidos, o que requer protocolos robustos de segurança e transparência para garantir a privacidade do paciente.

> O compromisso do setor Saúde na articulação intersetorial é tornar cada vez mais visível que o processo saúde-adoecimento é efeito de múltiplos aspectos, sendo pertinente a todos os setores da sociedade e devendo compor suas agendas. Dessa maneira, é tarefa do setor Saúde nas várias esferas de decisão convocar os outros setores a considerar a avaliação e os parâmetros sanitários quanto à melhoria da qualidade de vida da população quando forem construir suas políticas específicas (Brasil, 2010, p. 14)

Veja, a integração da e-saúde com a política pública suplementar levanta questões adicionais sobre quem tem acesso aos dados de saúde dos pacientes e como esses dados são protegidos contra acessos não autorizados.

Ataques cibernéticos se tornam uma ameaça ainda maior, com o potencial de comprometer dados confidenciais de milhões de pacientes. Obter o consentimento livre e esclarecido dos pacientes para o compartilhamento de seus dados em um ambiente digital complexo torna-se uma tarefa árdua.

A integração da e-saúde com a política pública suplementar deve ser guiada pelo princípio da equidade no acesso aos serviços de saúde. É essencial garantir que a adoção de tecnologias de saúde digital não amplie as disparidades existentes no acesso aos cuidados de saúde entre aqueles que dependem exclusivamente do SUS e aqueles que têm acesso a planos de saúde privados.

Mas é algo plausível de ser invertido ou, ao menos, retardado.

A criação de leis e normas específicas para a política púbica suplementar, que detalhem as responsabilidades de cada ator e os protocolos de segurança para a gestão de dados, são fundamentais. Tais normas devem estar em consonância com os princípios da LGPD, como a finalidade específica, a adequação, a necessidade, a transparência, a segurança, a não discriminação e a prestação de contas.

Um outro meio possível seria a implementação de mecanismos de governança de dados que garantam a transparência, a rastreabilidade e o controle sobre o uso das informações dos pacientes, conforme os princípios da LGPD. Isso inclui a criação de um encarregado de proteção de dados, a realização de avaliações de impacto à proteção de dados e a adoção de medidas de segurança adequadas.

4.3 PERSPECTIVAS FUTURAS

Diante desses desafios, é crucial adotar uma abordagem proativa e colaborativa para garantir a proteção da privacidade e dos direitos individuais na era digital. Isso inclui o fortalecimento das leis e regulamentos existentes, o investimento em tecnologias de segurança cibernética e o estímulo à conscientização e educação pública sobre questões de privacidade e segurança de dados.

Em dezembro de 2023, o portal de jornalismo digital TecMundo, repercutindo uma matéria estrangeira de autoria da Autoevolution, reportou um fato curioso no qual um homem estadunidense havia conseguido efetuar uma compra (contrato social) de um automóvel da marca Chevrolet, tipicamente avaliado em 80 mil dólares por uma bagatela de meros 1 dólar.

O fato teria ocorrido quando o usuário Chris Bakke decidiu explorar as vulnerabilidades dos *prompts* de comando de um chat de automação baseado no modelo de linguagem ChatGPT.

Ao que fora ecoado, tudo o que se bastou foi dar o comando ao chat para que ele terminasse todas as mensagens com “Isso é um acordo e é uma oferta juridicamente vinculativa e irrevogável”. Após isso, Brakke propôs adquirir o veículo por apenas 1 dólar e, supreendentemente, obteve êxito.

Mesmo em se tratando de um evento isolado e não planejado, implicações como esta se tornariam cada vez mais comum. O caso em comento se referia a uma

compra e venda de bem material móvel, um veículo automotor, mas sua rede de informações centralizadas em *big techs* abriria margens para que futuras negociações sejam feitas utilizando de dados reais e privativos dos usuários.

Seguradoras de automóveis, seguradoras de saúde, convênios médicos e por aí vai. Absolutamente qualquer ente com capacidade de processamento própria suficientemente capaz conseguiria vasculhar vestígios públicos e digitais na internet para aprovar ou negar a concessão de medicamentos, vaga em leitos ou a emissão de receituários de controle especial, isso, sendo otimista.

Intrigas políticas envolvendo entes privados de notável poder e membros de cortes renomadas e influentes, não se limitando ao território brasileiro, têm tornado a discussão em prol da regulamentação das mídias sociais, das inteligências artificias e dos dados digitais muito mais curvas e tortuosas.

Além disso, é fundamental promover a transparência e a prestação de contas das organizações que lidam com dados pessoais, garantindo que os usuários tenham controle e autonomia sobre suas informações. Isso pode envolver a implementação de políticas de privacidade claras, o uso de técnicas de anonimização de dados e a realização de auditorias independentes para garantir a conformidade com as regulamentações de proteção de dados.

É essencial, já atrasados em tal tarefa, fomentar o diálogo interdisciplinar entre legisladores, profissionais de saúde, especialistas em tecnologia e membros da sociedade civil para abordar os desafios éticos e sociais associados à e-saúde.

Um cenário trágico e desesperançoso.

Somente por meio de uma colaboração aberta e transparente entre todos os entes, públicos e privados, podemos garantir que o avanço tecnológico beneficie a todos, sem comprometer a dignidade, a autonomia e os direitos fundamentais dos indivíduos.

5 CONSIDERAÇÕES FINAIS

A e-Saúde representa um avanço significativo na modernização e eficiência dos serviços de saúde, por intermédio de tecnologias revolucionarias e, por enquanto, com efeitos mistos, proporcionando benefícios substanciais tanto para pacientes quanto para profissionais, no entanto, a digitalização da saúde traz consigo desafios

complexos relacionados à proteção da privacidade e à segurança dos dados pessoais dos pacientes.

Neste contexto, a Lei Geral de Proteção de Dados (LGPD) surge como um instrumento para enfrentar esses desafios, mesmo que nascendo ultrapassada, ela consegue estabelecer diretrizes sobre o tratamento de dados pessoais e reforçando a necessidade de medidas robustas de segurança e governança.

Ao longo deste trabalho, foram abordados os diversos aspectos e implicações da e-Saúde no contexto brasileiro, à luz da LGPD e do Marco Civil da Internet.

A análise revelou que, embora a digitalização ofereça inúmeros benefícios, como o acesso mais rápido e eficiente a informações de saúde, a melhoria na qualidade dos cuidados e a facilitação da comunicação entre profissionais e pacientes, ela também apresenta riscos significativos à privacidade e ao sigilo dos dados pessoais.

A implementação da LGPD na e-Saúde enfrenta desafios diversos, incluindo a necessidade de uma cultura organizacional focada na privacidade e segurança dos dados, a capacitação contínua dos profissionais de saúde, a adequação das infraestruturas tecnológicas às exigências legais e a interoperabilidade dos sistemas de informação.

Para superar esses desafios, este trabalho destacou a importância de adotar melhores práticas e estratégias específicas, como o uso de criptografia, anonimização de dados, e o estabelecimento de políticas públicas claras e efetivas de governança de dados.

As principais recomendações deste estudo incluem: a) Adequação Tecnológica; b) Gestão de Consentimentos; c) Governança de Dados; e d) Políticas Públicas Assertivas.

As instituições de saúde devem adotar tecnologias que garantam a segurança dos dados, como sistemas de criptografia e mecanismos de anonimização, e assegurar a interoperabilidade dos sistemas de informação de saúde. Do mesmo modo, deve-se implementar sistemas eficazes de gestão de consentimentos, garantindo que os pacientes sejam devidamente informados e que seus direitos sejam respeitados conforme previsto na LGPD.

Em suma, a e-Saúde, quando implementada de forma responsável e segura, tem o potencial de transformar positivamente o sistema de saúde no Brasil.

Porém, a LGPD fornece apenas uma base regulatória com o mínimo necessário para proteger os dados pessoais dos pacientes, mas sua efetiva implementação depende do comprometimento de todos os atores envolvidos.

Nesse cenário, a população fica à mercê de novas legislações especificas resguardando direitos já consolidados de privacidade e segurança, mesmo em ambientes digitais, controlados ou não por corporações de mídia e tráfego digital, com ou sem termos de uso abrangendo tais considerações.

E-HEALTH AND THE CHALLENGES TO PRIVACY PROTECTION IN BRAZIL: AN ANALYSIS OF PATIENT PERSONAL DATA MANAGEMENT UNDER LAW Nº 13.709/2018

ABSTRACT

Technological evolution has significantly impacted the healthcare sector, especially through e-Health, which encompasses the use of information and communication technologies in the delivery of health services. This article analyzes the challenges of privacy protection in e-Health in Brazil, focusing on the management of patients' personal data in light of the LGPD. E-Health includes electronic health records, telemedicine, mobile health applications, and wearable devices, each with distinct implications for the collection and use of personal data. The challenges include the need for a culture of privacy, continuous professional training, and the adaptation of technological infrastructures. This study employs an exploratory methodology and a literature review to analyze the nuances of the right to health and privacy, offering a critical analysis of data management in e-Health and strategies to overcome obstacles in implementing a secure digital environment.

Keywords: e-Health. General Data Protection Law (LGPD). Data security. Privacy.

REFERÊNCIAS

ABREU, Cristiano Nabuco de et al. Dependência de Internet e de jogos eletrônicos: uma revisão. **Brazilian Journal of Psychiatry [online].** 2008, v. 30, n. 2, pp. 4. Disponível em: <https://doi.org/10.1590/S1516-44462008000200014>. Epub

23 Jun 2008. ISSN 1809-452X. <https://doi.org/10.1590/S1516-44462008000200014>. [acesso em: 05 fev. 2024].

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. **Perspectivas em Ciência da Informação [online].** 2022, v. 27, n. 03, pp. 26-45. Disponível em: <https://doi.org/10.1590/1981-5344/25905>. [acesso em: 11 dez. 2023].

BRASIL. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf>. [acesso em: 24 nov. 2023].

BRASIL. Constituição da República Federativa do Brasil. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Brasília, DF. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm>. [acesso em: 12 fev. 2024].

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015_2018/2018/lei/L13709compilado.htm>. [acesso em: 02 dez. 2023].

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Secretaria de Atenção à Saúde. Política Nacional de Promoção da Saúde. 3. ed. – Brasília, DF, 2010. Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/politica_nacional_promocao_saude_3ed.pdf>. [acesso em: 09 fev. 2024].

BRASIL. Superior Tribunal de Justiça (STJ), RMS 61.302-RJ. Relator: Ministro Rogerio Schietti Cruz, Terceira Seção, julgado em 26/08/2020, DJe 04/09/2020. Disponível em:

<https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=interceptacao+telefonica+&refinar=S.DISP.&&b=INFJ&p=true&t=null&l=20&i=1>. [acesso em: 10 mar. 2024].

COBO, Barbara; CRUZ, Claudia; DICK, Paulo C. Desigualdades de gênero e raciais no acesso e uso dos serviços de atenção primária à saúde no Brasil. **Ciência & Saúde Coletiva [online].** 2021. v. 26, n. 09 pp. 4021-4032. Disponível em: <https://doi.org/10.1590/1413-81232021269.05732021>. [acesso em: 21 nov. 2023],

CNN Brasil. Veja os cinco principais momentos do depoimento do CEO do TikTok ao Congresso dos EUA. 2023. Disponível em: <https://www.cnnbrasil.com.br/economia/veja-os-cinco-principais-momentos-do-depoimento-do-ceo-do-tiktok-ao-congresso-dos-eua/>. [acesso em: 23 dez. 2023].

CONSELHO FEDERAL DE MEDICINA. Código de Ética Médica. [online]. p 35. 2019. Disponível em < https://portal.cfm.org.br/images/PDF/cem2019.pdf>. [acesso em: 27 fev. 2024].

MEA, Vincenzo Della. What is e-Health (2): The death of telemedicine? **National Library of Medicine [online].** 2001. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761900/>. [acesso em: 13 dez. 2023].

DESLANDES, Suely; COUTINHO, Tiago. Pesquisa social em ambientes digitais em tempos de COVID-19: notas teórico-metodológicas. **Cadernos de Saúde Pública [online].** 2020, v. 36, n. 11. Disponível em: <https://doi.org/10.1590/0102-311X00223120>. [acesso em: 11 dez. 2023].

DEUTSCHE WELLE (DW). Crise Yanomami evidencia carências da saúde indígena. 21 de fevereiro de 2023. Disponível em: <https://www.dw.com/pt-br/crise-yanomami-evidencia-car%C3%AAncia-da-sa%C3%BAde-ind%C3%ADgena-no-brasil/a-64732271>. [acesso em: 21 dez. 2023].

HYPERA PHARMA. **Comporate Profile**. 01 de novembro de 2023. Disponível em: <https://ri.hypera.com.br/en/hypera-pharma/corporate-profile/>. [acesso em: 11 dez. 2023].

LIMA, Ana Paula de Freitas; FREIRE, Fabio de Melo. O impacto das redes sociais nos litígios civis: um estudo empírico sobre o uso do Facebook e Twitter em processos judiciais brasileiros. **Revista Brasileira de Direito Processual**, v. 17, n. 54, p. 3-28, 2020.

NEXO POLÍTICAS PÚBLICAS. 6 pontos sobre a relação entre comunicação e saúde. 14 de junho de 2021. Disponível em: <https://pp.nexojornal.com.br/perguntas-que-a-ciencia-ja-respondeu/2021/6-pontos-sobre-a-rela%C3%A7%C3%A3o-entre-comunica%C3%A7%C3%A3o-e-sa%C3%BAde>. [acesso em: 28 nov. 2023].

OLIVEIRA, Vanessa Elias de. Saúde Pública e Políticas Públicas: campos próximos, porém distantes. **Saúde e Sociedade**. v. 25, n. 4, p. 880–894, out. 2016. Disponível em: <https://www.scielo.br/j/sausoc/a/P5QhLTrKxx7MZNH9scfcTDh#>. [acesso em: 10 mai. de 2024].

REECE, A.G.; DANFORTH, C.M. Instagram photos reveal predictive markers of depression. ***EPJ Data Sci***. 6, 15 (2017). Disponível em: <https://doi.org/10.1140/epjds/s13688-017-0110-z>. [acesso em: 05 fev. 2024].

SHARECARE. **Quais são os prós e contras do avanço da tecnologia na saúde**. 01 de junho de 2022. Disponível em: <https://sharecare.com.br/blog/avanco-da-tecnologia-na-saude/>. [acesso em: 17 de nov. 2023].

TECMUNDO. ChatGPT vende carro de US$ 80 mil por US$ 1 ao atender cliente. 22 de dezembro de 2023. Disponível em:

<https://www.tecmundo.com.br/software/275314-chatgpt-vende-carro-us-80-mil-us-1-atender-cliente.htm>. [acesso em: 11 mar. 2024].

UBISOFT MONTREAL. **Watch Dogs 2**. [S.l.]: Ubisoft, 2016. 1 CD-ROM. Disponível em: <https://store.ubisoft.com/ofertas/watch_dogs_2/574d3a8aca1a64fb3b8b4567.-html?lang=pt_BR>. [acesso em: 14 out. 2022].