CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA

CURSO DE GRADUAÇÃO TECNOLÓGICO EM REDES DE COMPUTADORES

ERISTON MATHIAS GONÇALVES

JOÃO VICTOR VICENTE DOS SANTOS

SEGURANÇA DE REDES: MELHORIA NA PROTEÇÃO DE ARMAZENAMENTO DE DADOS EM CLÍNICAS E HOSPITAIS BRASILEIROS ATRAVÉS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

G635s Gonçalves, Eriston Mathias

Segurança de redes: melhoria na proteção de armamento de dados em clínicas em clínicas e hospitais brasileiros através da lei geral de proteção de dados (LGPD) / Eriston Mathias Gonçalves, João Victor Vicente dos Santos. - Recife: O Autor, 2022.

36 p.

Orientador(a): Valfrido Filho Leite Filho.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2022.

Inclui Referências.

1. Lei Geral de Proteção de Dados. 2. Segurança. 3. Armazenamento de dados. I. Santos, João Victor Vicente dos. II. Centro Universitário Brasileiro - UNIBRA. III. Título.

CDU: 004

ERISTON MATHIAS GONÇALVES

JOÃO VICTOR VICENTE DOS SANTOS

SEGURANÇA DE REDES: MELHORIA NA PROTEÇÃO DE ARMAZENAMENTO DE DADOS EM CLÍNICAS E HOSPITAIS BRASILEIROS ATRAVÉS DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro - UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: Valfrido Filho Leite Filho

Co Orientadora: Ameliara Freire Santos de Miranda

RECIFE/2022

Dedicamos este trabalho aos nossos familiares que nos apoiaram desde o início da nossa graduação e aos professores responsáveis pelo nosso mergulho no conhecimento.

AGRADECIMENTOS

Agradecemos a Deus por nos ter dado sapiência para resolver todos os percalços que apareceram no caminho, sem fé a ansiedade nos dominaria.

Aos nossos orientadores Valfrido Filho Leite Filho e Ameliara Freire Santos de Miranda, pela inferência e diretriz sempre muito positiva para o nosso desenvolvimento.

Aos professores Filippo César Guedes e Marco Antônio dos Santos Guimarães, pelas correções, dicas e pela paciência.

À nossa família que respeitou o nosso isolamento para tornar esse trabalho possível, fazendo o que estava ao alcance deles para nos ajudar.

A todos que direta ou indiretamente, nos ampararam academicamente.

"A primeira igualdade é a justiça".

*(**Victor Hugo**)*

RESUMO

Ataques cibernéticos são antigos, porém, a proteção de dados não, para isto foi lançada a Lei Geral de Proteção de Dados, em 2018, e que após o crescente número de invasões na era pandêmica, em 2020, resultou em seu cumprimento absoluto pelos hospitais, clínicas e demais setores da saúde. Estar em conformidade com à lei nos protege quanto a invasões, mas não somente isto, afinal estamos em conformidade com a Constituição Federal Brasileira, que garante a individualidade e a não descriminalização de pessoas, seja por conta de sua cor, raça ou por deter alguma doença que vá, de alguma maneira, penalizá-lo socialmente. Destaca-se, ainda, a finalidade do uso dos Dados, seu armazenamento e a segurança imposta na área de saúde, em prol da observância e na contenção da multiplicação dos dados sensíveis dos titulares ou responsáveis. Conclui-se que a Lei veio para oferecer o sigilo necessário garantindo individualidade, segurança e limitações do uso dos dados.

Palavras-chave: Lei Geral de Proteção de Dados. Segurança. Armazenamento de dados.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

A linguagem é um dos signos tecnológicos mais antigos. Foi a partir dela que alicerçamos a base dos nossos conhecimentos. Comunicar-se e transmitir informações nos torna quem somos: uma sociedade compartilhadora, uma teia iniciada de forma solitária e comunica para outras teias; que se junta às demais distribuindo a gnose da nossa cultura. Falar em teia, nos remete a um fazer primário, e para vislumbrar nossa temática, chamaremos a teia de rede: uma interligação individual e coletiva que permite a troca, a evolução, união e promete para aquele que se mantém em rede- do que for, seja social, econômica, tecnológica- a convivência e a experiência de estar no mundo, em tribo, sociedade, do partilhar humano.

Assim como a linguagem, estar em rede nos irrompe o viver em comunidade e compartilhar informações extremamente necessárias para nossa evolução como ser humano, dotado de sapiência, em acordo ou desacordo com o que está sendo exposto, ainda assim evoluindo, repartindo. É mister destacar essa ideia de rede pois nos damos conta de que algo também depende de nós para ser formado, dos resultados ou da falta destes para o coletivo, e nesta que mora a decisão: partilhar ou não partilhar com outrem?

Filosoficamente, discordando do que diz Confúcio: “A experiência é uma lanterna dependurada nas costas que apenas ilumina o caminho já percorrido”.[1] Inferimos que o erro do passado, a experiência que ganhamos, ilumina o futuro e não o que já caminhamos, como sugere Confúcio.

Partilhar ou não pequenas informações pode levar à diversos problemas dentro desta rede e até em que ponto poderá chegar estes fios é a grande questão. A vantagem de saber partilhar ou não vem da experiência, o que nos faz liar alguns fatos, como por exemplo: na Primeira Guerra Mundial, a sociedade e as instituições americanas não deram a devida atenção ao conhecimento da língua falada pelos seus inimigos,

[1] Frase do filósofo chinês Confúcio ou K’ung-Fu-tzu (551-479 a.C.) disponível em: https://www.pensador.com/frase/MzEzNw/#:~:text=A%20experi%C3%AAncia%20%C3%A9%20uma%20lanterna%20dependurada%20nas%20costas,ilumina%20o%20caminho%20j%C3%A1%20percorrido.

passando por esta experiência de perda, já na Segunda Guerra Mundial, deram a devida atenção e saíram vitoriosos.

Cientistas e pessoas comuns- militares, no nosso exemplo- se aliam para fazer parte desta rede de experiências e dão margem a uma nova teoria, a Behaviorista, na qual compreende que o comportamento humano é ditado por estímulos externos. De acordo com o psicólogo behaviorista Burrhus Frederic Skinner (1904-1990), a linguagem pode ser considerada um comportamento que se desenvolve através da imitação e automatização, sempre acompanhadas do reforço positivo do meio. Partindo deste estudo temos a explicação para a vitória dos Estados Unidos na Segunda Guerra Mundial: a lanterna se acendeu ao conhecimento linguístico e desvendaram os códigos. Iluminaram o passado de derrota, analisaram os pontos em que erraram e estimularam as mudanças cabíveis no ataque além dos armamentos.

Ocasionalmente, os códigos e as redes não devem ser conhecidos por outrem, afinal, se existem códigos e codificadores é para manterem dados guardados, supostamente seguros de invasores. Esse percorrido sobre a linguagem foi justamente feito para que se estimasse o valor não somente de um dos primeiros signos tecnológicos, mas principalmente das redes atuais. Na contemporaneidade quando falamos de rede, lembramos das redes sociais como Twitter, Instagram, Facebook, LinkedIn, entretanto, dever-se-ia tomar em conta que a própria internet é uma rede interligada e internacional. Sendo interligada por computadores e que por meio desta, materiais como bases (doadas, cedidas, de elaboração própria) e informações, transitam para qualquer usuário que esteja conectado a mesma, sendo de qualquer lugar do mundo, por conseguinte: internacional.

> “A história da criação e do desenvolvimento da Internet é a história de uma aventura humana extraordinária. Ela põe em relevo a capacidade que tem as pessoas de transcender metas institucionais, superar barreiras burocráticas e subverter valores estabelecidos no processo de inaugurar um mundo novo. Reforça também a idéia de que no processo de que a cooperação e a liberdade de informação podem ser mais propícias à inovação do que a competição e os direitos de propriedade.” (CASTELLS, 2003, pág. 13)

Não queremos desmerecer a internet e seu uso, e sim alarmar o quão expostos estamos ao usarmos simples ferramentas de armazenamento de dados. É mister ressaltar que os invasores não são indivíduos que apareceram na geração Z ou Y, remonta à geração Baby Boomers, como sugere o Juíz Emanuel Alberto Sperandio Garcia Gimenes, em uma publicação na Revista de Doutrina TRF4:

> "O aparecimento dos primeiros casos de crimes informáticos data da década de 1960, e estes nada mais eram que delitos em que o infrator manipulava, sabotava, espionava ou exercia uso abusivo de computadores e sistemas." (GIMENES, 2013)

As ações criminosas feitas por esses invasores, chamados de *hackers*, tem aumentado significativamente, e os crimes cometidos vão de roubo de arquivos à sequestro de dados, geralmente enfrentados por grandes redes de empresas, cometidos principalmente na época em que assolava o COVID-19[2] e o alto uso e compartilhamento de dados via internet entre empresa-funcionário e funcionário-usuário/cliente.

O armazenamento de dados é uma faca de dois gumes em que ou entrega prestígio à instituição que consegue deixá-los a salvo, ou melhor, àquela que não sofre nenhum tipo de invasão de dados, não deixando seus clientes e a própria instituição desprotegida ciberneticamente ou é perdida a seriedade e a segurança que o nome da instituição passa aos usuários/clientes.

Partindo da premissa que a medicina é uma área de bastante prestígio aos seus trabalhadores – ou deveria ser, por cuidarem de vidas-, todo o seu sistema (seja ele institucional, de atendimento, políticas internas) deve versar para a segurança de todos os envolvidos, principalmente no tocante à saúde deles. Eticamente, é mister ressaltar que o Juramento Médico é claro quanto à confidencialidade e o respeito a privacidade do paciente, até mesmo em simples pesquisas, como se pode ver na Resolução 466/2012 do Conselho Nacional de Saúde é notável que é de suma importância o sigilo nesta área.

[2] Segundo reportagem da Folha de São Paulo, do dia 27 de junho de 2021.

Tendo em vista a Lei Geral de Proteção de Dados, que iremos abreviar e chamar de LGPD, de número 13.709, de 2018, objetivando proteger principalmente os direitos da liberdade e privacidade social (bem como juridicamente) surgiu para padronizar a regulamentação e as práticas que envolvem a proteção dos dados pessoais em todo o território nacional e em conformidade com o que já existia internacionalmente. A LGPD é uma inspiração da Legislação Europeia, que anela salvaguardar a autodeterminação do indivíduo, a transparência, a verificação e a responsabilidade pelos dados.

A ideia é impor limites ao acesso, compartilhamento, captação e uso dos dados, resguardando os direitos fundamentais dos usuários; haja vista que a Constituição Federal de 1988 assegura a partir do art. 5º, § 2º[3] o princípio da dignidade da pessoa humana, que consagra-se como direito à liberdade individual e que consequentemente, se estes forem violados, expõem-se a individualidade humana. Este indiviso do ser, também encontramos na Lei 13.709/2018, no seu artigo 1º que destaca, em consoante, no artigo 2º, versando sobre o regulamento da proteção de dados pessoais, fundamentando-se como o livre desenvolvimento da personalidade, ou seja, resguardar o que é seu.

Queremos realizar uma reflexão de como a LGPD pode mudar os dados no sistema de saúde, se for aplicado corretamente. É mister destacar que é comum a todas as áreas nos depararmos com novas normas, leis, regulamentações e obviamente à novas tecnologias e suas implicações em nosso cotidiano. Com a medicina não seria diferente, mesmo que apenas em atendimentos e não em pesquisas voltadas para a área tecnológica. Em clínicas e hospitais sérios, que se preocupam com seus bancos de dados, ainda se discute sobre esta nova lei, bem como todas as empresas que estão se adaptando para cumprirem-na e se livrarem de multas que podem chegar a ser bastante altas. Entretanto, dever-se-ia lembrar que nenhuma lei é imposta para complicar ou impedir a outrem de seguir sua vida/afazeres, e sim, evitar possíveis problemas futuros. No caso que estamos fazendo um recorte, em uma clínica ou hospital, é imprescindível para um melhor

[3] Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

atendimento ou decisão de procedimento a ser feito, essa consulta aos dados do paciente e que não seja violado nenhum direito, sendo mantidos e tratados com a devida segurança e consentimento do paciente.

E para estar em acordo com a LGPD, as clínicas e hospitais necessitam um sistema de prontuário desenvolvido já pensado em evitar possíveis multas, desenvolvidos em *Compliance,* ou seja, em conformidade com as exigências ditadas pela implementação da nova lei, cumprindo todas as políticas, regras, diretrizes e regulamentações propostas, sendo no seu armazenamento, no processamento e até como estas informações chegam através de *SMS*, *E-mail* ou *Chat* próprio do consultório ou hospital. Ocorrendo vazamento de dados, juridicamente, a clínica, hospital ou profissional da saúde poderá responder por violação da intimidade, da honra e da imagem de dado paciente.

Um profissional muito importante entre o coletador de informações sobre o paciente e o titular destes dados, é o *Data Protection Officer* (DPO) ou em português "encarregado", que faz esse elo dos dados coletados com as determinações pré-estabelecidas pela LGPD, evitando problemas como ciberataques, vazamentos e uso inadequado destes dados. Este funcionário deve orientar a equipe e resolver quaisquer problemas correlacionados.

A autorização do compartilhamento de, por exemplo, exames via e-mail ou com acesso via site da instituição, deve ser sempre consentido pelo cliente/paciente/responsáveis, bem como as decisões sobre terapias e procedimentos, de forma transparente, com os lados benéficos e maléficos deste compartilhamento. E tudo isso tem correspondência com o Termo de Consentimento Livre e Esclarecido (TCLE), que já é algo corriqueiro dentro das relações estabelecidas por médico-paciente. Sendo incumbência dos profissionais deixar claro para os responsáveis ou pacientes qualquer dúvida sobre a LGPD ou o TCLE, inclusive sobre o compartilhamento internacional dos dados obtidos pela clínica ou hospital.

2. JUSTIFICATIVA

Consideramos ser um tema relevante pelo fato de fazer parte do nosso cotidiano e não darmos a devida atenção, não apenas pela falta de alfabetização digital do nosso país (inclusive dos “bem letrados”) mas também por ser um tema atual e que está sendo analisado e estudado pelos profissionais interessados.

A falta de conhecimento deságua em consequências desagradáveis para os hospitais e clínicas- limite que estabelecemos para o tema- como a sua segurança e a da nossa cartela de clientes, evitando imbróglios futuros com o vazamento de informações e consequentemente da privacidade. Afinal, como explica DONEDA (2011, p. 94):

> “(...) a informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa maior privacidade a menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encera toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade”.

O profissional de Rede de Computadores é responsável pelo funcionamento das redes de computadores, tanto fisicamente como logicamente, além de promover integração, otimização, desempenho e segurança de redes. Atualmente, nós, profissionais desta área, somos fundamentais para fazer acontecer a relação dos nossos clientes com quem eles desejam alcançar. Sendo um tema de ampla busca pelas empresas, futuras utentes destes labores.

Nada mais justo do que pensar e versar sobre as Leis de Segurança de Dados e a consequente proteção de armazenamento de dados nas clínicas e hospitais brasileiros. O imbróglio que pode resultar na não proteção de dados já é uma justificativa plausível para o profissional da área estar antenado à esta temática atual, afinal o sistema de saúde é todo integrado, ou seja, se o paciente sofreu um acidente, é provável que ele precise ir em diversos segmentos daquele hospital,

como setor de urgência, traumatológico, cirúrgico e estes precisam do banco de dados do paciente. E ainda, se for transferido para outra unidade. Os dados estarão mais suscetíveis à invasão, afinal serão repassados via internet.

A tecnologia nos cerca em todos os âmbitos da nossa vida e é diante disto que é preciso haver mudanças, buscar informações relevantes sobre o tema e aplicá-las corretamente. É de muita utilidade saber leis e concatená-las com o nosso ofício tecnológico, afinal a intensificação da concorrência e o aquecimento do mercado tecnológico é exigente e os melhores profissionais devem estar capacitados para desmistificar a “dificuldade” na aplicação da LGPD.

3. PROBLEMATIZAÇÃO E OBJETIVOS

Objetiva-se a descrição da importância que tem a LGPD para a proteção do armazenamento de dados, bem como a relevância do investimento em segurança de dados. De maneira concisa iremos abranger o problema de vazamento de dados cadastrais em clínicas e hospitais e descrever a situação atual da LGPD neste nicho.

Vale ressaltar que qualquer atendimento em clínicas ou hospitais envolvem a participação de diversos profissionais, como médicos, enfermeiros, fisioterapeutas, além de especialidades diferentes; resultando para o paciente o deslocamento para diferentes lugares, como sala de ambulatório, de UTI, sala de cirurgia, sala de Raio-X etc. E para tal, inúmeras informações são captadas sobre o mesmo, até mesmo para dar continuidade ao tratamento prescrito, acumulando assim diversas informações, e quanto mais delas, mais referências são geradas e de diferentes dados, e para evitar a perda ou diferentes averiguações destes se torna necessário organizá-los, compondo apenas um banco de dados, seguro, límpido, organizado e que servirá de apoio para essa escolha de deslocamento do paciente, trazendo um atendimento humanizado, individualizado e seguro para ambos.

É mister ressaltar o problematizado até aqui com o que diz o autor Marciano (2006) que devido à grande complexidade da segurança, para se manter seguro é necessário ter atenção à configuração de todos os níveis de usuários e aos sistemas. Mas a preocupação com as pessoas, como havíamos mencionado anteriormente, não deixa de ser plausível, afinal, como nos esclarece Goldim e Francisconi (2005) em um hospital de grande porte, durante uma internação, até 75 pessoas diferentes chegam a lidar com o prontuário de um paciente. Além de que os pacientes devem autorizar o uso desses dados e o compartilhamento entre médicos e instituições.

Pela grande movimentação nos plantões e clínicas, e a consequente enorme corrente de informações confidenciais, precisamos aumentar a segurança destas, compartilhando mensagens criptografadas, ou seja, codificadas.

Antigamente, os prontuários médicos eram feitos à mão, todos organizados em grandes e pesadas pastas, podendo ser perdido parte ou todo de seu conteúdo e resultando na falta de agilidade. Nós fizemos a pergunta: Como a LGPD poderia melhorar a proteção desse armazenamento de dados e preveni-los contra seus usos indevidos?

Segundo Oliveira (2012), a tecnologia tem um papel de destaque no fazer medicina e no atendimento ao paciente, o que resvala na qualidade e agilidade de procedimentos clínicos e cirúrgicos, assim como nos diagnósticos. A tecnologia foi evoluindo e chegou às clínicas e hospitais e a utilização do prontuário eletrônico do paciente (PEP), segundo o autor Costa (2001) tem algumas vantagens e desvantagens, como por exemplo: as clínicas podem usar simultaneamente os dados, fica disponível o acesso remoto, evita-se falar o mesmo diagnóstico ou conter mais de uma vez a mesma informação sobre o estado do paciente, entretanto, a desvantagem seria o alto valor de investimento pra treinamento, *hardware*, *software*, resistência dos usuários e das próprias empresas. Porém, não é algo que se tenha mais tanta resistência, apenas é necessário cuidado com seu uso indevido, ou seja, o vazamento deles. A partir disso entra o conhecimento da LGPD pela empresa final – hospital, clínica- e do CDO, para a prevenção e proteção do armazenamento dos dados.

4. METODOLOGIA

Esta pesquisa é um estudo explanatório, o que segundo Malhotra (2001), tem como um dos objetivos possibilitar uma maior aproximação e entendimento do problema ao pesquisador, para que se consiga construir hipóteses mais adequadas**.** E envolverá levantamento bibliográfico e pesquisas que estimulem a compreensão do tema.

Além de descrever o que é a LGPD, e como se dá essa melhoria de armazenamento de dados em clínicas e hospitais brasileiros, o que nos traz nominalmente como pesquisa descritiva, como finalidade, segundo Mattar (1999), a descoberta e observância dos fenômenos, para posteriormente descrever, classificar e interpretar, sem modificá-lo ou interferir no mesmo.

Finalmente, é uma pesquisa feita através de levantamento de dados, estudo de Leis e que busca organizar, fundamentar e trazer conhecimento à comunidade acadêmica acerca da temática, e que fique claro a qualquer pessoa que se interessar pela temática, mesmo não sendo da área.

5. REFERENCIAL TEÓRICO

5.1 UMA INTRODUÇÃO À HUMANIZAÇÃO DA TECNOLOGIA

Conforme o que havíamos explanado na introdução, esta “sociedade em rede” está sendo profundamente invadida pela multiplicação da produção de dados, direcionando até mesmo as decisões ou a falta delas no meio de empresas, sites e da política, por meio da “indústria de banco de dados” (SOLOVE, 2004, p.19). Atuando no favorecimento da circulação dos dados comercializados ou irradiado por delegação, na grande maioria das vezes, de forma oculta, sem o consentimento ou conhecimento do usuário. Em consequência, um dos desafios é a interoperabilidade, ou seja, a troca de informações e dados entre computadores, a execução de programas que conversam entre si e que não possuem decodificação dos dados. Para ficar mais claro, a interoperabilidade pode ser compreendida em duas dimensões: do ponto de vista da informação ou pela maneira como os sistemas e softwares se comunicam entre si. (BRASIL, 2010).

Como podemos constatar, a tecnologia não é apenas relacionada às máquinas, e esta afirmativa está sendo fincada a partir do livro ‘O conceito de tecnologia’, do filósofo Álvaro Vieira Pinto, no qual é dissertado quatro sentidos ligados ao uso do conceito de tecnologia, sendo estes permeando no âmbito das artes, da teoria, das discussões técnicas e da ciência, das profissões, nas formas de produção etc.

. Álvaro Pinto (2005) ainda aponta que:

> “(...) toda tecnologia, contendo necessariamente o sentido, já indicado, de logos da técnica, transporta inevitavelmente um conteúdo ideológico. Consiste numa determinada concepção do significado e do valor das ações humanas, do modo social de realizar-se, das relações do trabalhador com o produto ou o ato acabado, e sobretudo envolve a ligação entre o técnico, em seu papel de fabricante de um bem ou autor de um empreendimento, e o destino dado àquilo que cria. A técnica representa o aspecto

> qualitativo de um ato humano necessariamente inserido no contexto social que a solicita, a possibilita e lhe dá aplicação (…).

Por todos esses aspectos temos a tecnologia, no sentido da teoria da técnica, sendo obrigada a se submeter ao social, as implicações humanas. Haja vista o exposto, a tecnologia deve servir ao humano e respeitar a sua natureza, leis, regras e diretrizes e, para tal, no campo de ação elegido neste trabalho, a tecnologia está sendo comandada pela entrada da LGPD. Sendo assim, rechaça-se a ideia de “máquinas” e humanizamos a ciência do ponto de vista da situação de segurança no armazenamento de dados, afinal é a teoria fazendo-se presente no realizar profissional e na força de produção.

5.2 IMPLEMENTAÇÃO DA LGPD

Antes de falarmos sobre a implementação da LGPD (Lei nº 13. 709/ 2018) vamos relembrar que ela regulamenta a proteção de dados no âmbito nacional, aliando a proteção do titular dos dados, o interesse público e impulsionando a amplificação econômica e tecnológica conectada à circulação da informação. Vale ressaltar que seu funcionamento implementado necessita de ajustes para a total proteção dos dados do titular, dos colaboradores e das empresas da área de saúde, como as clínicas e hospitais. Estes ajustes são necessários pois, conforme já havíamos comentado anteriormente, esses dados que foram gerados são compartilhados diversas vezes, dependendo dos setores que o paciente titular dos dados for relocado.

O processo não é tão simples, porquanto necessita de diversos passos, entretanto a lei em si é de fácil compreensão, mas é necessário ter um apoio jurídico para auxiliar tanto à empresa quanto o profissional DPO. Entender e estudar o ciclo de vida dos dados, regulamentar e padronizar a segurança de informação, auditar e monitorar o ambiente, criar um relatório de impacto à proteção de dados pessoais e criar um plano de ação para emergências, são etapas segundo Daniel Donda (2020) de suma importância para à adequação da lei.

O profissional DPO – Encarregado de Tratamento de Dados-, é responsável pelo cumprimento das regras de proteção de dados e torna-se referência para o exercício de direitos por parte dos titulares. (SOMBRA, 2019). Quanto as etapas dessa implementação, observemos a imagem a seguir:

Figura 1: Ciclo de vida dos dados, de acordo com o Art. 5º da LGPD

Fonte: Xpositum, 2022

O ciclo de vida dos dados consta de 7 etapas e explanaremos rapidamente como devem ser vivenciadas, em concordância com a LGPD: a coleta deve obedecer ao princípio da necessidade e da finalidade, isto é, os dados informados devem ser apenas os necessários para dar procedimento ao atendimento e ter a finalidade de identificar quem é o sujeito. Só pode ser feito o processamento em consonância com o artigo 7º da LGPD, e isso significa que precisa ser legitimado caso seja necessário o repasse ou até mesmo a reutilização destes dados na própria clínica ou hospital. A etapa de análise diz respeito a obediência dos princípios de tratamento, como propósito legítimo, específico e explícito. A quarta etapa, o compartilhamento, deve ser autorizada e consentida através de assinatura do titular dos dados ou de familiar responsável, a quinta etapa, do armazenamento, diz respeito ao prazo estabelecido definido. Tal como, se o paciente já realizou todos os procedimentos e está de alta médica, dever-se-ia ausentar o que há armazenado nos dados do hospital ou clínica os dados do titular ou responsável, sejam eles clínicos ou sociais; isto é, se findou sua

funcionalidade. A sexta etapa é a de reutilização, no caso, quando houver mudança de finalidade quanto ao armazenamento dos dados deste titular ou de seu responsável. E a última etapa depreende-se na eliminação após o término de seu tratamento.

Guiando-nos, ainda, pelas etapas propostas por Donda (2022) temos a elaboração de um Plano de Segurança da Informação (PSI), que deve garantir, segundo o autor: confidencialidade, integridade, disponibilidade, autenticidade e legalidade. E o que isso quer dizer? Que para gerar a PSI, deve existir a garantia de que somente pessoas autorizadas tenham acesso aos dados, sendo criptografados e caso necessite, exista a permissão aos recursos online. Além de não ser modificado nenhum dado, deveria existir um plano de desastre visando o resgate de todos estes dados, caso haja qualquer imbróglio e obvio, regulamentado, legalizado, assim sendo, dentro das normas previstas pela Lei.

Algumas das etapas vistas na imagem 1, tem a ver com esse PSI, e queremos destacar uma que nos leva à criação de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) de extrema importância e que deve ser atrelada ao uso de *Firewall*/IPS e também da DLP (*Data Loss Prevetion*) e da SOC, segundo alguns especialistas. Em que a primeira solução é para não permitir a invasão aos computadores, a segunda – DLP- é mais um reforço para o não vazamento de dados e a última, segundo a definição encontrada no Quadro Nacional de Referência para a Cibersegurança de Portugal, um SOC é:

> “um centro de operações de segurança, é tanto a equipa, que frequentemente opera em turnos de 24h/7 dias da semana, como as instalações dedicadas e organizadas para prevenir, detetar, avaliar e responder a ameaças e incidentes de cibersegurança, e para avaliar e cumprir com a conformidade das leis locais em vigor”.

O SOC pode evitar que hackers sequestrem informações em troca de um resgate milionário, por exemplo, ou ainda, observar movimentações dissonantes na parte financeira do hospital ou da empresa. Geralmente se faz uso de um SOC remoto, em que as empresas partilham para baratear o custo, afinal o SOC local exigiria um alto

investimento e o remoto, por ser fora da empresa, por mais que estejam vivendo um desastre naquela região, os computadores e consequentemente o armazenamento de dados estarão a salvo de qualquer tipo de problemática.

Não iremos fazer um grande recorrido de programas ou na PSI, mas é mister pontuar algo sobre os dados, muitas vezes se pensa que as informações elencadas em um hospital ou clínica são apenas relacionados a informações cotidianas: nome, sobrenome, endereço, CPF, RG, profissão, entretanto, há outros dados a mais, principalmente em ambiente hospitalar que é informado e armazenado. Estes outros dados, como orientação sexual, religião, etnia, dados genéticos, biométricos, filiação à partidos, ou sindicatos, saúde, entre outros, são chamados dados sensíveis. É evidente que a LGPD visa proteger transgressões das características ou do conjunto de atributos que formam a projeção da pessoa humana (BITTAR, 2015, p. 1). Por isso, a LGPD propende a observância da “(...)boa-fé e os princípios da finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas” (BRASIL, 2019). Com isto, depreende-se que os dados pessoais, para a LGPD, têm a ver com qualquer informação que possa ser relacionada com o indivíduo, a fim de identificá-lo, tolhê-lo, porém, não passando por cima de outras leis, como confere no art. 4 da LGPD, em que os dados podem ser liberados a fim de uma investigação ou até mesmo repressão por problemas penais.

5.3 DADOS SENSÍVEIS E FINALIDADE DO TRATAMENTO

Figura 2: Diferentes dados

Fonte: Opice Blum

A imagem nos explica as diferenças entre os dados pessoais e os dados sensíveis e como as empresas podem usar os mesmos, com anonimato ou pseudônimo. E reintegramos à luz da LGPD o que eles entendem por dados sensíveis: “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” (art. 5º, II). Este artigo possui por característica o princípio da não discriminação, resgatando a ideia de uma outra lei conhecida pelos setores jurídicos das empresas: a chamada de Lei de Cadastro Positivo, de nº 12.414/11.

O italiano Rodotà (2008, p.56) ressalta que estes dados pessoais, mesmo que não sejam os ditos ‘sensíveis’: “(…) podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada

quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas". Tal como os dados serem repassados para uma seguradora de carros e o paciente atendido- portador dos dados- é um jovem, até seus 35 anos, e que se feriu ou foi agredido dentro de uma casa de shows e mora em uma periferia de uma das cidades mais violentas do Brasil; com esta informação, a seguradora poderia discriminar o portador dos dados.

E que em acordo com o dito por Celina Bodin e Chiara de Teffé (2016, p.21): "entidades privadas e governamentais tornam-se capazes de "rotular" e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações, principalmente se analisados dados sensíveis".

Identificando a conjectura de tratamento aplicável as situações específicas de processamento de dados por hospitais e clínicas, dever-se-á verificar se estão em conformidade quanto à LGPD. Para isso, identifica-se a finalidade do tratamento, devendo ser informado ao titular o tratamento, a que se destina essa continuidade de dados, quais as providencias que serão tomadas para comunicar ao titular, garantir que o tratamento de dados será informada apenas para o que foi informado e quaisquer mudanças será informado para o portador de dados, ao planejar a forma de tratamento vai se limitar o uso mínimo de informações necessárias, garantindo a consecução das finalidades informadas; além disso, definir antecipadamente os mecanismos e processos executados nesses dados de maneira facilitada e gratuita, garantindo, assim, qualquer alteração da abrangência de compartilhamento sendo comunicadas ao titular. E os dois últimos procedimentos é a verificação quanto a exatidão, o acerto, e a utilização dos dados do titular, mantendo-se fiel à finalidade de tratamento informada e por último, observar a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento[4].

[4] Pensado em consonância ao Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD), disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

Conforme foi explanado, a finalidade do tratamento é larga, porém, iremos fazer um recorte quanto ao tratamento de dados pessoais dos pacientes e suas regras segundo a LGPD.

5.4 TRATAMENTO DE DADOS PESSOAIS DOS PACIENTES E SUAS REGRAS

Um grupo de advogados do CHC Advocacia[5], em seu blog, destaca que, quanto à implementação da Lei nos estabelecimentos de saúde:

> "(...) é permitido o tratamento de dados pessoais, também, para: a) a realização de estudos por órgão de pesquisa; b) a proteção da vida ou da incolumidade física do titular ou de terceiros; e c) para a tutela da saúde, sendo essa última possibilidade aplicada exclusivamente a procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

Como vimos, a lei não é feita apenas de proibições, também há as exceções, o problema é o desconhecimento da LGPD perante os usuários, e que são um número considerável de pessoas. Segundo dados do Instituto de Estudos da Saúde Suplementar (IESS), em março de 2021, existiam mais de 47 milhões de beneficiários de convênios médicos no nosso país, considerando a quantidade de habitantes, isso representa 22,5% da população. O que torna o SUS o Sistema de Saúde que mais abarca a população brasileira. Ou seja, não estamos tratando apenas de dados de adultos e sim, também de menores de idade, e estes devem ter seus dados recolhidos mediante a autorização (consentimento) específica dada pelo pai, pela mãe ou pelo responsável legal.

E acrescentando: o compartilhamento não se dá apenas entre a mesma clínica, afinal, em busca de mais uma opinião, os médicos compartilham os laudos de exames e outras informações com a finalidade de fechar um diagnóstico mais preciso, compartilhar experiência com outros médicos etc. Isso não deixará de existir, porém,

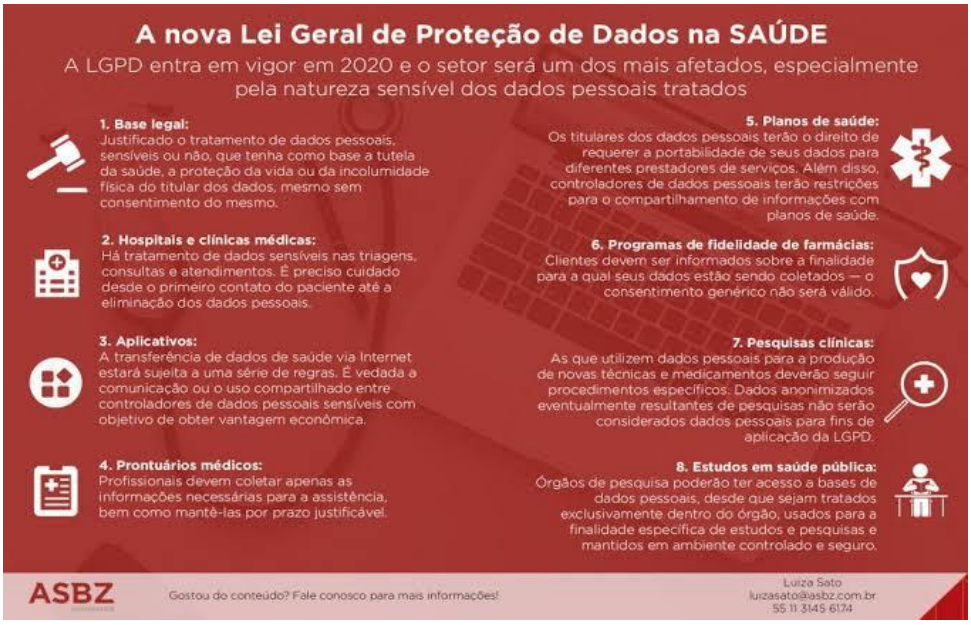
[5] https://chcadvocacia.adv.br/blog/lgpd-nos-estabelecimentos-de-saude/

há que adaptar algumas destas práticas e para isso que a LGPD foi lançada, afinal esta lei não versa apenas sobre os prontuários virtuais, mas todo e qualquer dado sobre o paciente.

A LGPD veio assegurar que o hospital, laboratório, clínica ou qualquer ambiente médico não compartilhe informações dos pacientes com seguradoras de vida, como por exemplo uma reavaliação de sinistro de um contrato, ação que só iria beneficiar à empresa e dar prejuízo ao usuário titular dos dados. Este exemplo está, inclusive, no § 5º do art. 11, que proíbe as operadoras de assistência à saúde o tratamento ou recolhimento de dados de saúde para essa pré-seleção de riscos na contratação ou exclusão de pacientes/usuários. Como é importante essa Lei para assegurar o bem-estar do paciente até mesmo em termos legais e o beneficiar com os direitos.

Além do benefício direto ao titular dos dados, a empresa que se compromete a seguir a LGPD, fica livre de problemas como: prejuízo financeiro, uma vez que fora da conformidade se prevê sanções que variam de advertência multas que podem chegar em 2% sobre o faturamento e calculado por infração, inclusive penalidade diárias, de acordo com o art. 52 da LDPD. Prejuízo quanto à sua reputação, que tanto falamos ao longo desta pesquisa, o que pode ser um dano fatal à imagem da empresa, causando até mesmo a sua falência ou perda de ganhos diários e com este percalço, mais uma, a comercial, dificultando parcerias e possíveis investimentos.

Figura 3: A nova Lei Geral de Proteção de Dados na Saúde



Fonte: ASBZ Advogados

Na figura 3, podemos ver um resumo do que tratamos aqui quanto à segurança desses dados, a sua aplicabilidade e o acesso para órgãos públicos de pesquisa, como por exemplo o que aconteceu no ano pandêmico. É importante destacar que o titular dos dados precisa informá-los legalmente e assinar o Termo de Consentimento de dados, geralmente é declarado assinalando o consentimento e a concordância mais a assinatura do usuário ou, se for online, esse consentimento se dá por assinalar bem como pela confirmação dos dados, comumente, apenas inserindo o endereço eletrônico na página web ou aplicativo. Permanecendo obrigatório aos agentes de tratamento de dados a segurança destas informações, mencionado no artigo 46, §2º, deve ser observada desde a concepção das informações até o seu uso. Este é um conceito de proteção da privacidade que chamam de *Privacy by Design*, caracteriza-se por medidas proativas, que antecipa e evita eventos invasivos de privacidade, muito importante para que não vaze a anamnese dos pacientes findado o tratamento.

6. VAZAMENTO DE DADOS

Nesta pesquisa de 2019, vemos que o maior setor acometido pelo vazamento de dados, no mundo, foi na área da saúde, representando 27%, seguido por 14% em instituições financeiras.

Figura 4: Vazamento de Dados por Setor

Fonte: ACPD Brasil, 2019

É frente a este dado alarmante, que viemos alertar a importância da segurança quanto à estes dados, não somente por conta dos prejuízos já citados anteriormente, (financeiros, através de multas e retaliações que a empresa venha a ter em investimentos e na diminuição dos clientes), mas os problemas jurídicos que pode enfrentar, não somente a empresa, mas o funcionário responsável pela segurança, como constatamos no Art.42: “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais,

é obrigado a repará-lo". Isto significa que se o titular dos dados sofrer algum dano moral ou material por conta deste vazamento, quem arcará com problemas judiciais é o responsável pelos dados e a consequente falta de suporte e segurança oferecido a estes.

Como segue no Art. 43, da Lei de nº 13.709/2018:

> "Os agentes de tratamento só não serão responsabilizados quando provarem:
>
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros".

Obviamente que o titular de dados pode ir antes à empresa para tentar uma conversa com o setor jurídico, conseguindo reparar os ônus nesta relação, antes de enfrentar um imbróglio judicial. Para evitar ao máximo esse tipo de problema, o DPO (*Date Protection Officer*), deve saber como evitar os ataques.

6.1 CAUSAS DOS ATAQUES AOS BANCOS DE DADOS E COMO EVITÁ-LOS

Na era pandêmica e porque não dizer também nesta era pós-pandêmica, muito se falou e se tem falado sobre segurança cibernética, afinal o crescente uso da rede foi evidente: usuários fazendo home office (e consequentemente levando parte da empresa para casa), o atendimento médico via e-consulta (telemedicina), aumentou o número de compras por aplicativos e por URL, houve um aumento considerável do uso das redes sociais, de plataformas de streamings, enfim, uma infinidade de conexões estavam ao dispor. O uso da internet só faz crescer a cada dia e por esta razão se faz necessário saber quais as causas dos ataques aos bancos de dados e como evitar estar à mercê destes roubos, evitando surpresas desagradáveis.

Ainda endossando o aumento do uso da rede, em 2020 foram criadas 2428 vagas a mais na modalidade de teletrabalho, que correspondeu a 41% das oportunidades abertas em site de recrutamento e seleção (VICENTIN; LUCENA, 2021). Segundo uma pesquisa realizada pela Fundação Instituto de Administração (FIA) coletou, realizada em abril de 2020, com dados de 139 pequenas, médias e grandes empresas que atuam em todo o Brasil, observou-se que 46% delas adotaram o regime Home Office. 67% das companhias tiveram problemas na adaptação quanto ao Home Office, porém apesar das dificuldades, metade delas afirmou que essa modalidade superou as expectativas (MELLO, 2020).

O baixo custo de cometer um crime cibernético atrelado a outras facilidades é a grande causa dos ataques, afinal para se transformar em um “fora da lei”, basta ter um aparelho roteador (ou wi-fi) e um aparelho que dá acesso à internet, além de estar escondido por trás de uma tela, com pouca ou quase nenhuma visibilidade de descoberta de onde partiu o ataque (pois levam meses para investigarmos e fazer com que o crime seja penalizado perante a lei). Para toda a doença a sua cura, se os hackers conseguem decodificar páginas, aplicativos ou sites, isso significa que alguma brecha foi deixada e rastreada, por tanto, deve ser evitada e “fechada”, por meio de criptografia forte, controlando o acesso de pessoas aos dados e a permissão do acesso aos arquivos, importante ressaltar que isso tanto fisicamente como no aspecto virtual. Tendo em vista que os mal-intencionados surgem de todos os lados – funcionários, ex-funcionários, ataques digitais, é importante um monitoramento de ambos os espaços (físico ou digital).

De envio de dados até estafar o sistema, forçando-o a perder dados, na intenção de prejudicar à falsificação de URL para roubar os dados do usuário como login e senha para acessar o que estiver permitido e até mesmo tentar uma invasão mais massiva, ainda podendo quebrar senhas e chaves criptografas, os hackers são capazes de tudo e ficam sempre à espreita, buscando encontrar uma vulnerabilidade para vender dados na deep-web[6], para concorrentes, para outras pessoas mal-intencionadas, para praticarem outros crimes (uso de dados de cartão de crédito,

[6] Grosso modo é a internet profunda, oculta, que de alguma forma auxilia o anonimato e privacidade dos seus navegantes.

CPF, etc.) e até mesmo raptar dados e pedir um resgate, principalmente depois da Lei que versamos neste trabalho.

Imagem 5: Panorama das ameaças cibernéticas no Brasil

Fonte: Portal da Ilha (2022)

Investir em segurança é o ponto crucial para não ser vítima deste tipo de ataque digital. No caso de um hospital é de extrema importância, uma vez que diversas máquinas são ligadas à uma rede, como o de ressonância magnética, o computador no qual o médico envia para outro setor para que imprimam a receita médica, o exame etc. Lembrando que a segurança deve ser 24h por dia, os 7 dias da semana, protegendo-se contra malware, atualizando continuamente e constantemente as redes contra as diversas variantes de malware, ter um serviço de prevenção contra intrusos (IPS) para impedir que descubram a vulnerabilidade da rede, além de ter uma área restrita para enviar códigos. E consequentemente, um ambiente isolado em nuvem para analisar o sistema, segurança no e-mail para combater ataques, conforme

a imagem 5, de *spam*, cavalos de Troia, *phishi*, entre outros, além de aplicar contramedidas em *endpoints* móveis e remotos dentro e fora da rede; e muito importante: manter tudo atualizado, sempre. Estar em conformidade com a Lei de nº 13.709/2018 é estar protegido e proteger o cliente.

A LGPD visa que os dados pessoais sejam perpassados de forma confiável, assegurada entre os sistemas internos e externos, garantindo que os dados se mantenham confidenciais e não sejam rastreados por pessoas mal-intencionadas. A urgência no cumprimento da lei se fez notar quando na pandemia diversas empresas começaram a ter seus dados violados e o que foi pensado em 2018 (a lei), começou a fazer sentido de urgência em 2020, em uma entrevista[7] para o Portal *Focus.jor*, o advogado Fernando Santiago (2020) deixou claro que: "(...) os dados pessoais que antes eram tratados de forma quase artesanal pelas empresas, sem a devida atenção, passam agora ser tutelados pelo direito, razão pela qual devem ser manuseados com as condições estritas prevista na lei". Espera-se que hospitais, clínicas e demais especialidades da saúde estejam mais atentos e protejam os dados com afinco, uma vez que a força da lei está na sua execução.

[7] Essa entrevista tem como título "O setor público está preparado para LGPD?" e foi realizada pelo jornalista Frederico Cortez.

7. CONCLUSÃO

Não nos restam dúvidas quanto à urgência da implementação de segurança à ataques cibernéticos, conforme pedido pela Lei nº13.709/2018, afinal um plano de segurança das informações protegem não somente os usuários- titulares dos dados-, como a empresa, e melhor pagar a adaptação do sistema, um bom DOP e estrutura que pagar a multa que chega a ser por dia, além dos processos jurídicos que podem ser encarados pela vulnerabilidade dos dados e a reação do titular dos mesmos ou de seus responsáveis.

Estar em conformidade com a lei é dever de todo cidadão brasileiro e diz muito sobre a postura que uma empresa leva em consideração a seu país, seu ofício e aos seus envolvidos, sendo estes seus funcionários ou seus clientes. A aprovação da LGPD reforçará o endossamento de uma estrutura que findará os ataques cibernéticos no Brasil, ou pelo menos venha a diminuir o número de ataques.

Vale ainda ressaltar que o Estado deve promover medidas que se façam tornar possível a implementação desse sistema de segurança, promovendo palestras com as principais dúvidas quanto a finalidade da lei, da importância da proteção dos dados, implementar algum tipo de ação que venha abrilhantar o fazer jurídico da empresa, como proporcionar descontos em produtos, diminuição de impostos na compra de programas ou serviços que tenham como objetivo o cumprimento da lei, que sabemos ser de suma importância não somente para a proteção da empresa como da individualidade do ser.

REFERENCIAS

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8.ed., rev. aum. e mod. Por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BRASIL. **Conselho Nacional de Saúde**. [Internet]. Resolução nº 466, de 12 de dezembro de 2012.

Disponível: <http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>. Acesso em 10 de maio de 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. *Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).* Presidência da República, Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 de junho de 2022.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 18 de junho de 2022

_____. Ministério da Saúde. Secretaria Executiva. Departamento de Informática do SUS–Datasus. **Troca de informações em saúde baseada num framework integrado de conhecimento e comunicação.** Agosto de 2010. (mimeo).

_____. **Constituição da República Federativa** do **Brasil**, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03 /**constituição** /constituicaocompilado>. Acesso em 15 de junho 2022.

BRASIL. Conselho Nacional de Saúde. Resolução 466/2012. Disponível em: <http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>. Acesso em junho de 2022.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**; tradução Maria Luiza X. de A. Borges; revisão Paulo Vaz. – Rio de Janeiro: Jorge Zahar Ed., 2003

CORTEZ, F. **“O setor público está preparado para LGPD?**”. *Focus.Jor.* Disponível em: <https://www.focus.jor.br/o-setor-publico-esta-preparado-para-lgpd-por-frederico-cortez/>. Acesso em: 20 de junho de 2022.

COSTA, C. G. A. **Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas da World Wide Web e da Engenhar ia de Software**. Dissertação de Mestrado. Universidade Estadual de Campinas, 2001.

DONDA, D. **Guia Prático de Implementação da LGDP: Tudo o que sua empresa precisa saber para estar em conformidade**. São Paulo: Labrador, 2020.

DONEDA, Danilo. **Um código para a proteção de dados pessoais na Itália**. Revista Trimestral de Direito Civil, Rio de Janeiro, v. 16, p. 117, 2003.

FOLHA DE SÃO PAULO. **Sequestro de dados de empresas vira joia do cibercrime na pandemia.** Reportagem de junho de 2021.

Disponível em: <https://www1.folha.uol.com.br/mercado/2021/06/sequestro-de-dados-de-empresas-vira-joia-do-cibercrime-na-pandemia.shtml> Acesso em 14 de junho 2022.

GIMENES, E. A. S. G. 2013. **Crimes Virtuais**. Disponível em: <http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html.> Acesso em: 19 de junho de 2022.

GOLDIM, J. R.; FRANCISCONI, X. **Bioética Clínica**. 2005. Disponível em: < http://www.pucrs.br/bioetica/cont/carlos/bioeticaclinica.pdf> Acesso em: 20 de junho de 2022.

MARCIANO, J.L.P. **Segurança da Informação - uma abordagem social** – Brasília, 2006.

MALHOTRA, N.K. **Pesquisa de marketing: uma orientação aplicada**. 3.ed. Porto Alegre: Bookman, 2001.

MATTAR, F. N. **Pesquisa de marketing: metodologia e planejamento**. 5. ed. São Paulo: Atlas, 1999.

MELLO, D. **Home office foi adotado por 46% das empresas durante a pandemia**. Agência Brasil, 2020. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2020-07/home-office-foi-adotado-por-46-das-empresas-durante-pandemia> Acesso em 18 de maio de 2022.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. **Redes sociais virtuais: privacidade e responsabilidade civil**. Análise a partir do Marco Civil da Internet. Revista Pensar, v. 22, n. 1 2017.

OLIVEIRA, J. F. **Gestão de Tecnologias da Informação e da Comunicação na Saúde: uma análise sobre o uso do prontuário eletrônico**. Interface – Natal/RN – v.9 – n.1 – jan/jun 2012

PINTO, A.V. **O conceito de tecnologia**. Rio de Janeiro: Contraponto; 2005

PORTUGAL. **Quadro Nacional de referência para a Cibersegurança: Centro Nacional de Cibersegurança**. Disponível em:< https://www.cncs.gov.pt/pt/quadro-nacional/>. Acesso em: 16 de junho de 2022.

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

SOLOVE, Daniel. **The Digital Person. Technology and Privacy in the Information Age**. New York: New York University Press, 2004, p. 19.

SOMBRA, Thiago Luís Santos. **Fundamentos da Regulação da Privacidade e Proteção de Dados**. 1. ed. São Paulo: Revista dos Tribunais, 2019.

SKINNER, B.F. **O comportamento Verbal**. São Paulo: Cultrix/EDUSP, (1957), 1974.

VICENTINI, LUCENA. **Vagas de emprego em home office crescem 309% em 2020**. Olhar Digital, 2021. Disponível em: https://olhardigital.com.br/2021/03/06/pro/vagas-de-emprego-em-home-office-crescem-309-em-2020/. Acesso em 22 de junho 2022.