ESTUDO DE CASO SOBRE A APLICAÇÃO DA LGPD NA ÁREA DA PSICOLOGIA CLÍNICA

DA SILVA, Milton Machado Pereira [1]
MISAGHI, Dr. Mehran [2]

RESUMO

Com os avanços tecnológicos, uma quantidade maior de informações trafegam pela rede e os usuários são mais dependentes da mesma, porém, tem crescido muito a quantidade de incidentes relacionados a crimes digitais e vazamento de dados, com isso têm sido criadas novas leis de forma a tentar preencher essas brechas jurídicas, sendo que cada negócio tem sua particularidade quanto à adequação, como por exemplo a psicologia clínica, que muita vezes precisa armazenar dados pessoais e sensíveis de seus pacientes. Dessa maneira temos como objetivo geral do trabalho verificar a aderência a LGPD na área de psicologia, por meio de questionários a serem aplicados. Assim, a pesquisa possui um caráter bibliográfico e exploratório, realizado através de um estudo de caso. Como resultado temos que a maior parte dos registros dos pacientes são armazenados em arquivos, envolvendo informações da pessoa natural e a maior parte dos entrevistados não possui cópias de segurança ou plano de contingência em caso de indisponibilidade dos dados, apesar de 36,4% ainda não estarem adequados à legislação, 80% não utiliza boas práticas do tratamento dos dados, o que torna um grande desafio por parte dos gestores a adequação necessária conforme a legislação, treinamento dos colaboradores e implementação das práticas e políticas adequadas antes que se iniciem as multas que podem ser aplicadas pela ANPD, órgão fiscalizatório.

Palavras-chave: Segurança da Informação. LGPD. Psicologia.

1 INTRODUÇÃO

Com o avanço da tecnologia, as informações passam a ser moldadas e operadas cada vez de forma mais digital na sociedade, diminuindo o uso de meios físicos de armazenamento de informações e tendo como principal fonte de inserção de dados o próprio usuário dos dispositivos tecnológicos através da internet.

Porém, essa dependência pela tecnologia também trouxe alguns problemas tais como: sequestro de dados, furto de identidade, vírus, golpes diversos, enganar

[1]Graduando em Bacharelado em Sistemas de Informação
[2]Professor Doutor em Engenharia Elétrica.

Joinville – SC, 01 de Julho de 2021.

as pessoas para que forneçam dados pessoais, vazamento de dados, entre outros incidentes. Dessa forma, o CERT - Centro de Estudos e Respostas para Tratamento de Incidentes (2018) relata que com o aumento da difusão da Internet também aumentaram os incidentes reportados.

Como forma de tentar reduzir esses incidentes, foram criadas legislações que aumentam a penalidade para os crimes informáticos, sendo a mais atual a Lei Geral de Proteção de Dados Pessoais (LGPD), que entre vários detalhes tem como base a proteção dos dados pessoais e sensíveis dos titulares. A LGPD veio como uma resposta aos vários incidentes de vazamento de dados que estavam ocorrendo, conforme Pinheiro (2020), como por exemplo, o caso Cambridge Analytica (EL PAÍS, 2019) e o caso Edward Snowden (GRANATO, 2016), onde estavam sendo coletados dados de forma ilegal de milhares de titulares. Essa lei foi motivada pela GDPR (Regulamento Geral sobre a Proteção de Dados), criada pela União Européia em 2018, de acordo com Maldonado (2019).

Conforme as revoluções tecnológicas aumentam seu impacto social, problemas éticos aumentam. Então, como a LGPD é uma lei recente, espera-se que as constituições necessitem da criação de novas normativas quando as atuais já não abrangerem determinados serviços e aparatos tecnológicos, que modificam a forma como as tarefas são realizadas.

Diversas clínicas psicológicas mantém os documentos de pacientes armazenados em arquivos e pastas por não confiarem em meios tecnológicos, conforme Rousmaniere et al. (2014). Assim como existem clínicas que optam por guardar seus dados em nuvem ou outros meios virtuais justamente por achar que os dados estariam mais seguros. Nos dois casos, existe a oportunidade e necessidade de melhoria do armazenamento dos dados, no primeiro, por ser um meio antiquado e no segundo pelos dados poderem estar vulneráveis.

O que se destaca é que o problema de vazamento de dados torna-se ainda mais grave em se tratando de clínicas de psicologia, pois além do vazamento de dados pessoais tal como nome, número de telefone, endereço, entre outros, há ainda as informações sensíveis dos pacientes, mantidas pelos profissionais para auxiliar nas consultas e no acompanhamento do tratamento proposto.

Diante disso, tem-se como objetivo geral do trabalho realizar um estudo de caso sobre a aplicação da LGPD na área de psicologia clínica, verificando a posição das clínicas da área em relação ao assunto. Para isso temos os seguintes objetivos

específicos: identificar os meios de armazenamento de informações utilizados pelos profissionais da área e debater acerca da segurança e conformidade destes meios; discutir sobre o valor da LGPD na área proposta e apresentar seus conceitos e por fim, propor meios de implementação e adequação à LGPD.

2 REFERENCIAL TEÓRICO

Neste capítulo são apresentados os conceitos sobre segurança da informação, a legislação acerca de proteção de dados, dados pertinentes à psicologia clínica e a relação médico-paciente, e normas técnicas relacionadas. Conceitos estes, fundamentais para o entendimento do trabalho aqui proposto.

2.1 SEGURANÇA DA INFORMAÇÃO

De acordo com Vilaça e De Araújo (2016), a informação vem se tornando cada vez mais importante na sociedade, se moldando conforme a evolução da tecnologia e sendo também um recurso crítico para realização do negócio e execução da missão organizacional.

A informação é um recurso que agrega valor para a organização e deve ser bem gerenciado e utilizado, tendo em vista que é necessário garantir que ela esteja sendo disponibilizada apenas para aqueles que necessitam dela em um determinado momento. Assim a análise da informação deve ser realizada como um conjunto de dados que podem gerar informações tornando-se assim um ativo valioso para a organização.

Segundo Sudré (2018), a segurança da informação é a união dos três fatores, sendo eles: ferramentas, controles e políticas de segurança. A segurança da informação é caracterizada pela prevenção de três atributos básicos da informação, sendo eles: confidencialidade, disponibilidade e integridade.

1. Confidencialidade: Este termo define a garantia de que os dados estão sendo tratados em discrição e sem divulgação não autorizada ocorrendo desde a coleta, passando pela guarda e tratamento até o momento em que os mesmos sejam descartados ou mudem seu responsável. (HINTZBERGEN *et al.*, 2018);

2. Disponibilidade: A disponibilidade tem seu objetivo ligado ao fornecimento de acesso a uma informação no momento desejado. Ou seja, é a propriedade de que a

informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade no momento em que tenha sido requisitada, sendo válida para qualquer tipo de dado ou forma de acesso, desde que se tenha permissão para tal (SUDRÉ, 2018);

3. Integridade: A integridade pode ser caracterizada como uma forma de garantir que as informações não sejam alteradas ou violadas de forma indevida, segundo Sudré (2018). Dessa maneira, espera-se que a informação seja disponibilizada de forma completa e sem qualquer tipo de modificação, conforme HINTZBERGEN *et al.* (2018).

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi criada em 2018, entrando em vigor no Brasil no dia 18 de setembro de 2020 (BRASIL, 2018), seu objetivo é a regulamentação do tratamento de dados pessoais de clientes e usuários por parte de empresas públicas e privadas. A motivação para a criação da LGPD foram os constantes vazamentos de dados e os escândalos envolvendo dados pessoais.

A lei impacta na gestão de dados pessoais pelas empresas em todos os setores, fazendo com que as empresas implementem ou adequem novos procedimentos ou criem novos setores para alinhamento às novas normas (POHLMANN, 2019). Esta lei representa um novo marco no ordenamento jurídico brasileiro, tendo em vista que trata da proteção de dados pessoais independente do meio em que sejam adquiridos e independente de se referir à pessoa física ou jurídica.

A LGPD está dividida em 10 capítulos e composta por 65 artigos, e alguns deles ainda precisam ser complementados pela ANPD (Autoridade Nacional de Proteção de Dados) que está em processo de criação, e será esse órgão o responsável pela fiscalização, regulação e punição das instituições que não seguirem a legislação (BRASIL, 2018).

2.3 TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

A LGPD define de forma específica em seu art. 5º, no inciso II, a questão de dados pessoais sensíveis, ou seja, informações de origem política, racial, étnica, religiosa, dados com relação à saúde ou vida sexual, de biometria ou genética, quando vinculado à uma pessoa. A manipulação destes dados pode discriminar seu titular, portanto, são sujeitos a maior proteção.

2.4 DADOS PESSOAIS NA PSICOLOGIA CLÍNICA

Em análise aos termos condicionados na nova lei de proteção de dados surge a necessidade que todos os profissionais se adequem ao uso da mesma em seu dia a dia de atividades, assim se faz inclusão dos psicólogos, sendo que os mesmos realizam o armazenamento e coleta de dados de seus pacientes. Com isso, alguns pontos devem ser devidamente seguidos, desde a entrevista inicial com o paciente, demais sessões, até a manipulação do prontuário e diagnóstico (SADOCK; RUIZ, 2017).

Os dados são de responsabilidade de seu controlador (clínica ou profissional), que não pode compartilhá-lo com terceiros exceto mediante aprovação do titular ou quando necessário para prestação de serviços suplementares (BRASIL, 2018).

2.5 RESPONSABILIDADE CIVIL NO ÂMBITO DA PROTEÇÃO DE DADOS

A responsabilidade civil na proteção de dados é uma obrigação que provém de outra relação em que um erro primário foi cometido. Isso faz com que as companhias tenham que frequentemente passar por uma reavaliação dos seus termos de consentimento, cumprindo com os requisitos de informação, sendo uma das obrigações que possivelmente irão gerar dever de reparação de danos perante a lei, de acordo com Maldonado (2019).

Isso faz com que as empresas além de se adequar a legislação tenham que se manter em compliance com ela, revisando os processos que estão sendo feitos e trabalhando constante com treinamento e políticas de segurança da informação, de forma a evitar vazamento de dados e demais incidentes.

2.6 ISO 27002: CONTROLES DE SEGURANÇA DA INFORMAÇÃO

A norma ISO 27002 tem foco em boas práticas na gestão de segurança da informação, onde constam as políticas de SI, a gestão dos ativos (bens ou informações mais valiosas e que precisam ser protegidas), segurança em recursos humanos, segurança física, do ambiente e de operações e comunicações, gestão de tratamento de incidentes e continuidade dos negócios, controle de acesso e aquisição, manutenção e desenvolvimento de sistemas, entre outros.

A norma apresenta em seu teor uma estipulação para melhores práticas como o apoio da implantação do SGSI, definidas em diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as empresas, incluindo a escolha, a implantação e gerenciamento de controles, considerando os ambientes de risco de SI da organização. (27001, 2020).

3 METODOLOGIA

Nesta seção serão apresentados os procedimentos metodológicos necessários à elaboração dessa pesquisa e aquisição das informações para construção das conclusões obtidas, de forma a alcançar os objetivos que foram propostos no início do trabalho.

Para isso foram seguidas algumas etapas, como a obtenção do referencial teórico e a posterior construção de um estudo de caso referente ao tema proposto, tendo como finalidade o levantamento de informações que contribuíram para aprofundamento do tema, tornando essa pesquisa também exploratória, prática necessária para validação dos resultados.

3.1 CARACTERIZAÇÃO DA PESQUISA

Segundo Pádua (2019), a pesquisa baseia-se em dois tipos de procedimentos metodológicos, sendo eles: bibliográfico e de campo. O primeiro procedimento realizado foi o bibliográfico, onde procurou-se fazer um levantamento teórico acerca dos temas apresentados com base em livros, artigos e publicações feitas na área e o segundo, por meio do contato com os profissionais da área.

3.2 LOCAL DA PESQUISA

A pesquisa foi realizada com clínicas de psicologia e profissionais da área de forma a entender como eles estão se adequando às exigências da LGPD, tal como formalizar o consentimento dos dados pessoais, possuir políticas de segurança para lidar com essas informações e possíveis acidentes que podem ocorrer, tratamento dos dados durante todo seu ciclo de vida, entre outros.

3.3 ETAPAS DA PESQUISA

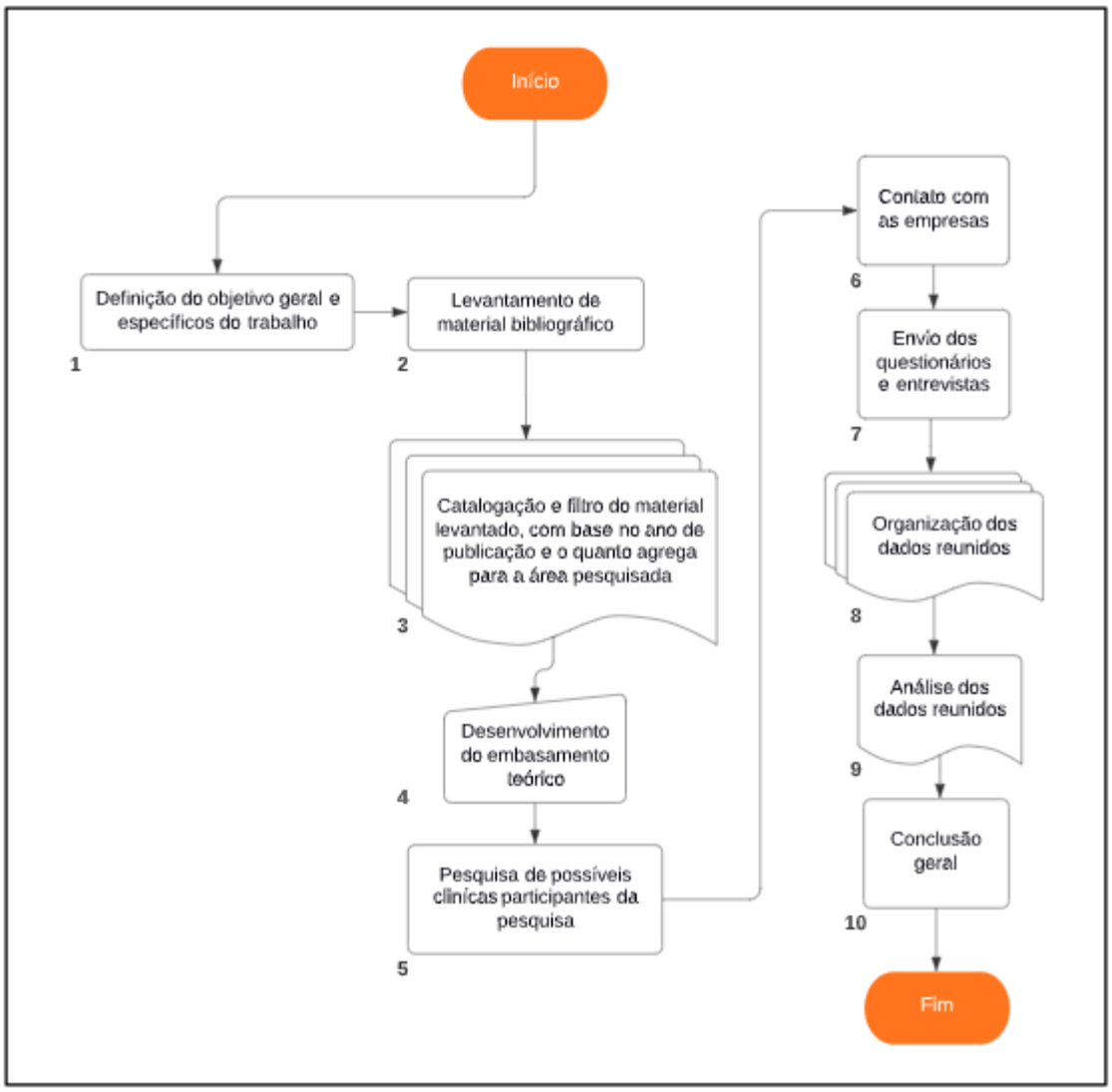
A pesquisa de campo foi desenvolvida através de questionários, que contemplam 7 questões de múltipla escolha e que foram aplicadas de abril/2020 a março/2021, onde foram obtidas respostas de 55 profissionais que trabalham em clínicas de psicologia.

Inicialmente, foi utilizado de publicidade online para tentar obter a atenção dos profissionais e que eles respondessem as questões, porém esse método não apresentou resultados significantes, sendo necessário entrar em contato com cada clínica e profissionais de forma individual, via telefone, e-mail e *whatsapp*.

Finalmente, a união da pesquisa bibliográfica com a de campo nos permite ter um conhecimento da situação com um todo, remetendo ao procedimento experimental e permitindo avaliar a forma como as companhias vão passar a trabalhar com os dados, e os riscos e mudanças que isso apresenta para sua área de atuação.

Com base nisso, demonstram-se as etapas que foram desenvolvidas na pesquisa na Figura 1, sendo que inicialmente definiram-se os objetivos que seriam realizados no trabalho, em seguida levantou-se o material bibliográfico, seu filtro e leitura, de forma a poder entender melhor o referencial que fundamentaria a pesquisa e que foi escrito. Em seguida foram pesquisadas as clínicas e profissionais dispostos a contribuir com a pesquisa e posterior envio dos questionários, para por fim, os dados das respostas serem organizados e apresentados.

Figura 1 - Fluxograma das etapas da pesquisa.



Fonte: do Autor (2021).

4 RESULTADOS E DISCUSSÕES

A pesquisa foi então realizada entre abril de 2020 a março de 2021, onde obteve-se a quantidade de respostas por período conforme Tabela 1, totalizando 55 respostas de profissionais que trabalham em clínicas psicológicas, sendo que todos os que responderam atuam na área de psicologia, psicoterapia ou psiquiatria.

Tabela 1 – Quantidade de respostas obtidas por período.

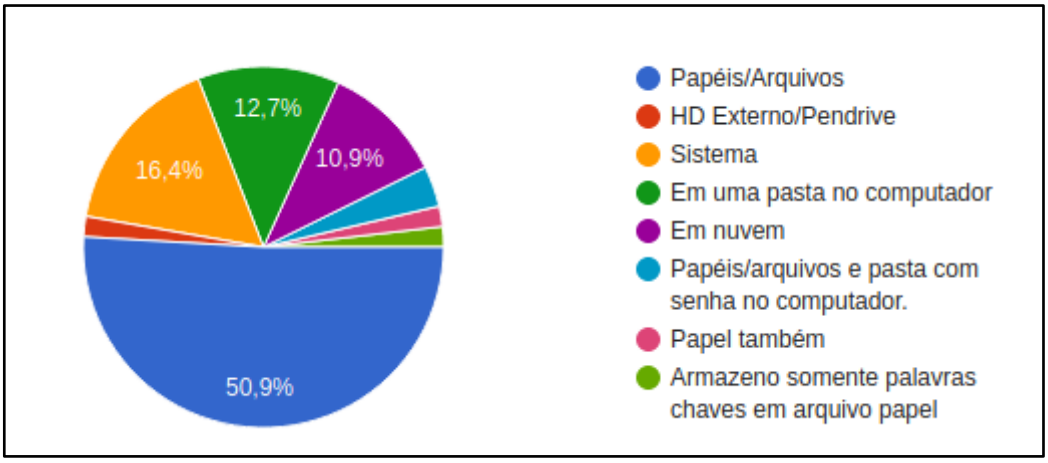
Período	Quantidade
04/2020	12
05/2020	1
12/2020	9
01/2021	33

Fonte: do Autor (2021).

Inicialmente foi questionado como são armazenadas as informações dos clientes/pacientes, onde a maior parte respondeu que armazena em papéis ou arquivos (50,9%), seguido por sistema (16,4%) e em uma pasta do computador (12,7%), conforme demonstrado na Figura 2. Desses, apenas 1,8% utilizam HD externo e pen drive ou arquivos com senha no computador, enquanto 10,9% armazenam essas informações na nuvem.

Ambos os resultados, tanto armazenamento em papel, computador ou na nuvem podem acarretar em grandes possibilidades de vazamento de dados, seja por perder as anotações, invasões de computador e sistemas ou demais incidentes relacionados à segurança.

Figura 2 – Respostas sobre como são armazenadas as informações dos clientes/pacientes.

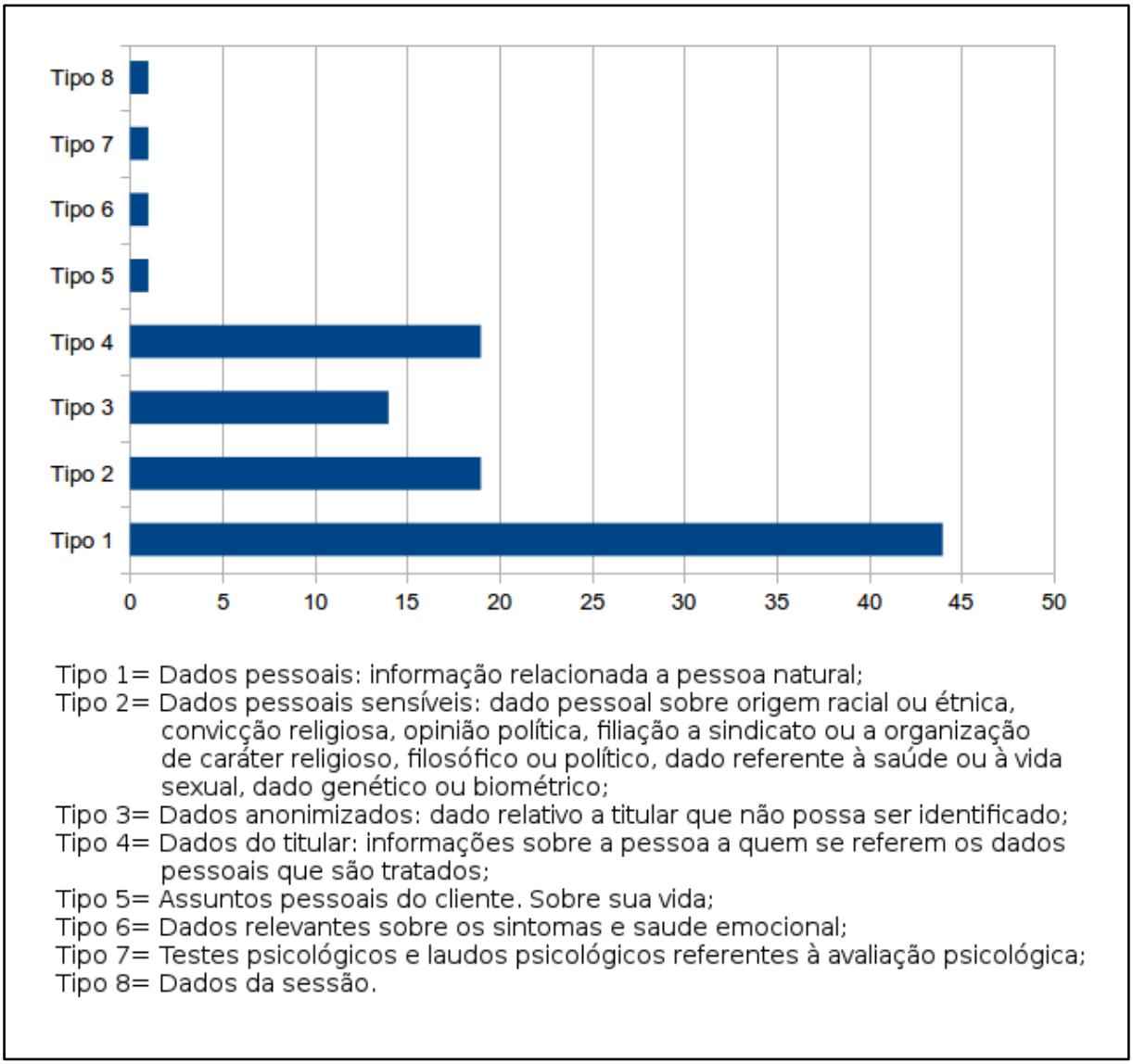


Fonte: Do Autor, 2021.

A questão três coloca em pauta o tipo de dado pessoal, onde 80% dos respondentes dizem armazenar informações sobre pessoa natural, o que inclui informações que podem identificar o indivíduo. Os demais, com 25,5% das respostas obteve-se o armazenamento de dados anonimizados e em seguida, com

1,8% cada, informações sobre a vida do cliente, testes psicológicos e laudos, dados da sessão e referentes à saúde emocional do cliente.

Figura 3 – Respostas sobre o tipo de dados pessoais que são armazenados.



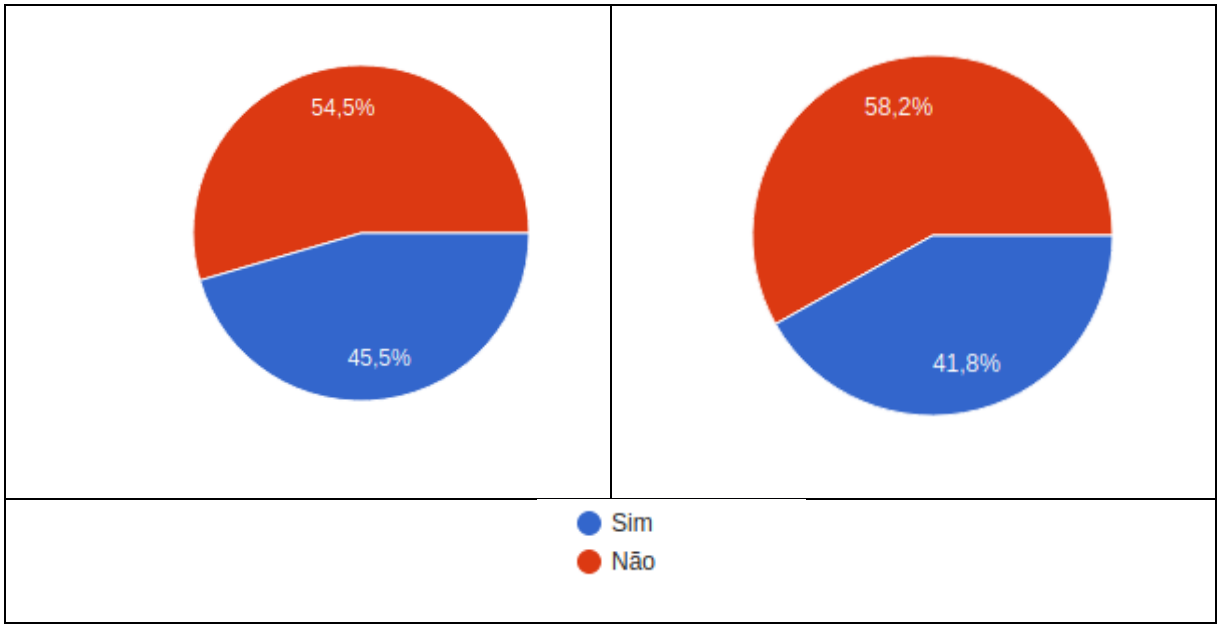
Fonte: Do Autor, 2021.

Na quarta pergunta é verificado se é mantida uma cópia dessas informações, e 54,5% respondeu que não, conforme Figura 4a. Em seguida, de acordo com as respostas apresentadas na Figura 4b, investiga-se se existe algum plano de tratamento de incidentes para caso os dados sejam perdidos, e 58,2% dos entrevistados responderam que não.

Essas duas perguntas abordam um elevado risco não apenas no dia a dia dos profissionais, que teriam grande dificuldade em continuar seus atendimentos sem as informações, mas também referente à LGPD, onde a empresa deve possuir

políticas de segurança implementadas e definidas, bem como medidas para minimizar os danos em caso de incidentes.

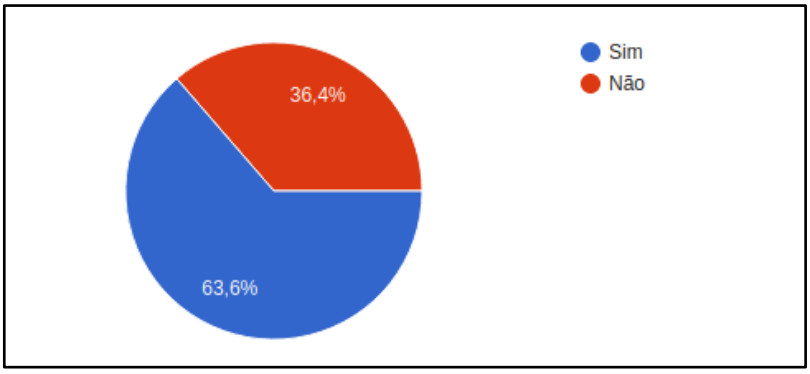
Figura 4a – Respostas sobre se é mantido uma cópia das informações; Figura 4b - Respostas sobre se existe um plano de contingência em caso de perda de informações.



Fonte: Do Autor, 2021.

A questão 6 investiga a existência de um consentimento para o tratamento de dados, já que a Lei Geral de Proteção de Dados já se encontra em vigor, porém ainda sem penalizações pela ANPD, porém essas empresas e profissionais sofrem risco de terem que responder judicialmente por ainda não estarem formalizando um consentimento. Como resultado obtém-se que 63,6% possui esse controle, o que demonstra que a maior parte já está se adequando à legislação, enquanto 20 dos entrevistados, o equivalente a 36,4% não possui essa formalização, conforme Figura 5.

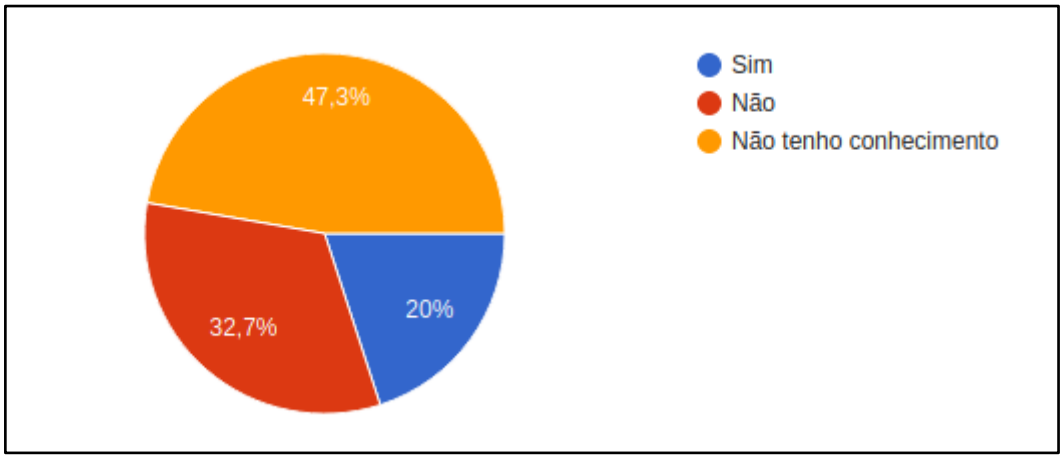
Figura 5 – Respostas sobre se é formalizado o consentimento para tratamento de dados.



Fonte: Do Autor, 2021.

Por fim, analisa-se se a empresa em que trabalham os entrevistados possui alguma política de segurança da informação ou governança para proteção de dados pessoais, e apenas 20% dos entrevistados, o equivalente a 11 pessoas, afirmaram que sim, conforme Figura 6, os demais ou não possuem conhecimento ou sabem que essa política não existe, o que, conforme já mencionado, pode fazer a empresa ou profissional responderem judicialmente por isso, conforme a LGPD, e caso não se enquadrem até Agosto de 2021 estão sujeitos a multas por parte da entidade reguladora.

Figura 6 – Respostas sobre se existem políticas de segurança ou governança para proteção de dados pessoais.



Fonte: Do Autor, 2021.

4.1 DISCUSSÃO

Finalmente, algumas soluções que podem ser propostas para enquadrar a aquisição e obtenção dessas informações de acordo com a LGPD são as seguintes: utilização de controle de acesso e chaves para os arquivos que são armazenados de forma física em papel, cópia digital das mesmas e utilização de backups incrementais diários para as informações que são armazenadas de forma digital, devendo o servidor de backup estar em outra rede e outro local físico do que o servidor principal.

Também é necessária a elaboração de um plano de contingência e restabelecimento dos serviços em caso de incidentes, bem como políticas de segurança da informação, que irão ser utilizadas por todos que têm acesso às

informações e que irão padronizar a forma com que as mesmas devem ser trabalhadas.

4.2 SÍNTESE DA PESQUISA

A maior parte das informações dos pacientes é armazenada em papéis e arquivos, o que os deixa vulneráveis a uma série de incidentes que podem comprometer as informações, além do acesso indevido. A maior parte dos dados armazenados são sobre a pessoa natural, o que em caso de incidente apenas iria expor o paciente, porém não seus gostos e preferências. A maior parte dos entrevistados não mantém uma cópia das informações nem plano de contingência em caso da sua perda, o que pode comprometer a realização do trabalho. Apesar de 36,4% dos entrevistados ainda não estarem adequados à lei, a maior parte já está se adequando à formalização necessária, porém 80% não tem ciência nem o hábito de cuidar da segurança dos dados, o que precisa ser feito em um prazo curto, tendo então as empresas a necessidade de criar políticas de segurança, implementá-las e ainda conscientizar seus funcionários.

CONSIDERAÇÕES FINAIS

O avanço tecnológico permitiu que a sociedade evoluísse em se tratando do armazenamento e uso dos dados, permitindo sua consulta com uma maior agilidade, principalmente ao se utilizar dispositivos conectados à internet. Porém, essa alta disponibilidade das informações trouxe problemas como roubo e vazamento de dados, vírus e outras pragas digitais, e diversos outros incidentes.

De forma a tentar reduzir esses incidentes foi criada a LGPD (Lei Geral de Proteção de Dados), inspirada na versão europeia da mesma, a GDPR, cujo objetivo é proteger os dados dos titulares e tratar as informações durante todo o seu ciclo de vida. Com base nisso, espera-se que as empresas se adequem a essa nova legislação, sendo que a lei já está em vigor, porém com as multas sendo aplicadas pelo órgão fiscalizador (ANPD) a partir de agosto de 2021, mas já com aplicação judicial.

Conforme o tipo de negócio da organização, sua adequação tem um diferente grau de complexidade, principalmente se há a possibilidade de tratamento de dados

sensíveis, tal como ocorre com clínicas psicológicas, onde dados de pacientes são mantidos tanto em documentos em papel quanto em registros no computador, sendo que os dois casos oferecem falhas e brechas de segurança que podem levar ao vazamento de dados pessoais e sensíveis dos pacientes.

Diante disso, o objetivo geral do trabalho foi de realizar um estudo de caso sobre a aplicação da LGPD na área de psicologia clínica, verificando a posição das clínicas da área em relação ao assunto, para isso foram analisados temas como segurança da informação e seus princípios de integridade, disponibilidade e confidencialidade; as particularidades da LGPD, sua forma de tratamento de dados e sua aplicação na psicologia clínica; a aplicação da ISO 27002 na segurança da informação.

O resultado final apresentado foi que 36,4% dos entrevistados ainda não estão adequados à legislação, sendo que 80% desconhece e não possui o hábito de cuidar da segurança dos dados, o que demonstra um desafio quanto ao pouco tempo para se adequar e implementar as políticas e treinamentos necessários.

Como trabalho futuro sugere-se refazer a pesquisa com as mesmas clínicas após o período de um ano, de forma a verificar se houveram mudanças quanto à adequação à lei e conhecimentos de proteção dos dados.

REFERÊNCIAS

27001. O que é a normal ISO 27001? Disponível em <https://www.27001.pt/>. Acesso em: 8 de setembro de 2020. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018, institui a **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 10. Set. 2020.

CERT. **Total de incidentes reportados por ano.** Disponível em <https://www.cert.br/stats/incidentes/>. Acesso em: 11 de agosto de 2020.

EL PAÍS: **EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários. [S. L.], 13 jul. 2019.** Disponível em: <https:// brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html>. Acesso em 10 de dezembro de 2020.

GRANATO, Daniela. **Caso Snowden**. 2016 Disponível em <https://danielaggranato.jusbrasil.com.br/artigos/394542311/caso-snowden>. Acesso em: 18 de novembro de 2020.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: com base na iso 27001 e na iso 27002**. 2. ed. Rio de Janeiro: Brasport, 2018.

MALDONADO, Viviane Nóbrega. **LGPD – Lei geral de proteção de dados – Manual de implementação**. Revista dos tribunais, 3ª tiragem. 2019.

PÁDUA, Elisabete M; **Metodologia da pesquisa: Abordagem teórico-prática**. Papirus, 1ª edição. 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**. Saraiva Jur, 2ª edição. 2020.

POHLMANN, S. **LGPD Ninja: Entendendo e implementando a Lei Geral de Proteção de Dados na Empresa**. Rio de Janeiro: Fross, 2019.

ROUSMANIERE, Tony; ABBASS, Allan; FREDERICKSON, Jon. (2014). **New Developments in Technology-Assisted Supervision and Training: A Practical Overview**. Journal of Clinical Psychology, n.70, p. 1-12, novembro. 2014. Disponível em: <https://www.researchgate.net/publication/265786216_New_Dev >. Acesso em: 04 ago. 2020.

SADOCK, Benjamin J.; SADOCK, Virginia A.; RUIZ, Pedro. **Compêndio de Psiquiatria: Ciência do Comportamento e Psiquiatria Clínica**. 11. Porto Alegre: Artmed, 2017.

SUDRÉ, Gilberto. **Curso de Sistemas de Informação**. Vincit. 2018.

VILAÇA, Márcio Luiz; De Araújo, Elaine Vasquez Ferreira. **Tecnologia, Sociedade e Educação na Era Digital.** Unigranrio, Duque de Caxias, RJ. 2016.