Adequação das Organizações à LGPD: Aspectos a serem considerados para evitar a Vulnerabilidade Humana na exposição indevida de Dados Pessoais

Hannibal Escobar R. H. De Carvalho (Universidade Candido Mendes)
Alberto Eduardo Besser Freitag (Universidade Candido Mendes)

Resumo
A privacidade e a proteção de dados são temas muito debatidos atualmente em virtude da nova Lei Geral de Proteção de Dados Pessoais (LGPD). A análise de risco e a segurança da informação são dois aspectos muito importantes que devem ser considerados pelas organizações para atenderem aos requisitos determinados pela lei. Com a imposição de multas para empresas que não se adequarem às obrigações da LGPD, as empresas que tratam com dados pessoais de funcionários, clientes e usuários se viram na obrigação de buscar se adequar aos artigos que especificam como proceder no tratamento dos dados. A proteção adequada da privacidade se baseia no controle de dados pessoais durante todo o seu ciclo de vida, que incluem descoberta, coleta, armazenamento, classificação, controles de acesso e monitoramento interno de ameaças, de forma a evitar a vulnerabilidade humana na exposição indevida de dados pessoais. O uso de tecnologia se torna quase que indispensável quando se trata de ações de segurança no tratamento de dados, porém, o fator humano também é fundamental. No âmbito desse contexto, o objetivo desta pesquisa foi identificar por meio de uma revisão sistemática da literatura baseada no protocolo PRISMA os aspectos que devem ser considerados por uma organização para se adequar à LGPD, a fim de evitar a vulnerabilidade humana na exposição indevida de dados pessoais. Do grande volume de registros identificados, incluíram-se 21 artigos na seção de fundamentação teórica, que subsidiaram a elaboração de uma proposta conceitual com aspectos relevantes a serem considerados por uma organização na adequação à LGPD, principal resultado deste trabalho.

Palavras-Chave: LGPD, organizações, proteção de dados, privacidade, vulnerabilidade.

1. Introdução

A comunicação constante entre dispositivos eficazes, sensores e pessoas está criando uma gama de dados que estão sendo processados e armazenados a cada momento (MAGRANI, 2018). Com a criação de regulações para proteção de dados pessoais e o crescimento acelerado na geração desses dados, é necessária uma mudança na forma como as organizações os tratam e os utilizam. Para dar conta da quantidade de dados que são gerados, as empresas precisam se adequar às melhores práticas para gestão e tratamento desses dados, a fim de evitar a vulnerabilidade humana na exposição indevida de dados pessoais.

Segundo Henein e Willemsen (2019) os regulamentos de privacidade em todo o mundo se desenvolveram mais nos últimos dois anos do que no século passado, apesar da demanda do consumidor por privacidade vir aumentando nas últimas duas décadas. A confiança está no nível mais baixo de todos os tempos, tornando insustentável a forma como os dados são manipulados atualmente. Os escândalos envolvendo a empresa britânica Cambridge Analytica e o Facebook em 2016, acusados de utilizar de forma indevida os dados pessoais dos usuários, para a criação de psicográficos com fins comerciais e políticos (POWER, 2019), motivaram a criação de um regulamento

europeu para proteção de dados pessoais. Com base nesse regulamento, em 2020, entrou em vigor no Brasil, a Lei Geral de Proteção de Dados Pessoais, a LGPD. Basicamente a lei prevê regras específicas para o tratamento de dados pessoais, nos meios digitais e físicos (BRASIL, 2018).

Publicado em 2016 com vigência a partir de 25 de maio de 2018, o Regulamento Geral sobre a Proteção de Dados ("*General Data Protection Regulation*" - GDPR), marca uma transição a partir da antiga Diretiva de Proteção de Dados Pessoais (95/46/CE), vigente na União Europeia (UE) desde 1995 (UNIÃO EUROPÉIA, 2016). O GDPR é o mais recente mecanismo da UE para mitigar o risco de privacidade, onde o impacto sobre um indivíduo é mais alto. O GDPR enfatiza a importância dos direitos de um titular de dados, a maneira pela qual as violações de dados são tratadas e o controle geral sobre dados pessoais. O impacto do GDPR vai muito além da UE, pois afetará todos os países que, de alguma forma, possuem empresas que atuam lá. O objetivo é garantir não só a privacidade de qualquer cidadão em solo europeu, mas também assegurar que empresas do continente realizem negócios apenas com empresas que respeitem esses direitos (IRAMINA, 2020).

As pessoas estão cada vez mais propensas a mudar para a concorrência se acreditarem que outro fornecedor manipulará melhor seus dados pessoais, tornando-as menos vulneráveis à exposição indevida dos mesmos. O resultado é um impacto cumulativo nos negócios que se traduz diretamente nos resultados de uma organização. Para piorar as coisas, as organizações veem a privacidade da mesma maneira que percebem a segurança - como uma troca entre funcionalidade ou puramente como um centro de custos (HENEIN e WILLEMSEN, 2019).

Pesquisas recentes apontam que a maioria das empresas no Brasil não tem conhecimento suficiente de quais dados pessoais, direta e indiretamente identificáveis, elas possuem, sejam eles dados estruturados ou não estruturados, localizados na nuvem ou em servidores físicos (SERPRO, 2019). Na maioria dos casos, os dados pessoais estão presentes em todos os sistemas, dificultando o controle do acesso a eles, quando definidos para a finalidade de processamento correta. Em situações assim, o primeiro passo é realizar uma avaliação de impacto na privacidade, identificando e classificando os dados. É importante frisar que a privacidade não é apenas uma tarefa necessária por meio da LGPD, ela é relevante na avaliação dos riscos envolvidos para atender o regulamento.

Com tantas tecnologias disponíveis, muitas organizações se veem sobrecarregadas com os requisitos de privacidade. Vale ressaltar que o desafio é proporcional à quantidade de dados manipulados, ao número de usuários e à complexidade do ambiente. As soluções de segurança necessárias devem abranger os recursos de descoberta, mapeamento, classificação, controles de acesso e monitoramento, pseudonimização ou anonimato e controles sobre todo o ciclo de vida dos dados sob sua responsabilidade (ALLAN, 2019).

Diante do contexto supracitado, surge a seguinte questão de pesquisa: "Quais aspectos devem ser considerados por uma organização para se adequar às definições e obrigações da nova lei, evitando assim a vulnerabilidade humana na exposição indevida de dados pessoais?". Para superar os desafios de controle que virão com a implantação da LGPD, será necessária uma mudança na forma de gerir os dados, o que justifica a realização deste estudo. Isso poderá evitar penalizações e multas desde a sua coleta até o seu armazenamento, visto que toda a cadeia de tratamento de dados é abordada na lei. Dessa forma, este trabalho tem como objetivo identificar os aspectos que devem ser considerados por uma organização para se adequar à LGPD e evitar a vulnerabilidade

humana na exposição indevida de dados pessoais, por meio de uma revisão sistemática da literatura.

A presente pesquisa está dividida em cinco seções. Além desta primeira seção introdutória, a segunda trata da fundamentação teórica na qual está baseada a pesquisa. A terceira seção explica os procedimentos metodológicos da pesquisa, uma revisão sistemática da literatura. A quarta apresenta os resultados e a análise das informações obtidas. A quinta seção aborda as considerações finais do estudo, seguida das referências.

2. Fundamentação teórica

A pesquisa buscou apresentar por meio de uma revisão da literatura uma síntese abrangente e coerente dos principais conceitos e contextos referentes à privacidade e à LGPD.

2.1. Privacidade

A preocupação com informações pessoais não é uma ação recente, ao longo da história em diversos momentos o homem manteve esse pensamento. A discussão sobre questões de privacidade é tão antiga quanto a humanidade. Começando com a proteção do corpo e da casa, logo evoluiu na direção de controlar as informações pessoais (LUKACS, 2016).

Para Holvast (2008), a história da privacidade deixa claro que há uma forte relação entre a privacidade e o desenvolvimento da tecnologia. O autor destaca que a discussão moderna começou com o uso de câmeras e passou a incluir o desenvolvimento e o uso de computadores em uma sociedade da informação na qual os dados pessoais de cada indivíduo são coletados e armazenados.

Não é apenas uma grande preocupação que a privacidade esteja em risco, deixando os serem humanos vulneráveis à exposição indevida dos seus dados pessoais, mas também que está sendo criada uma sociedade de vigilância. Essa perda de privacidade parece ser ainda mais importante, uma vez que a proteção da privacidade depende fortemente da vontade política de protegê-la. Dentro dessa concepção, Henein e Willemsen (2019) destacam os principais momentos e marcos na história recente, referentes à forma como a sociedade busca, de alguma forma, dar mais atenção à privacidade das suas informações.

- 1763 - O britânico William Pitt, Conde de Chatham, discursa na Câmara Comum sobre a revogação de um imposto especial de consumo que permitia buscas sem garantias. Nesse discurso ele fala em um tom mais forte a favor da privacidade de um indivíduo contra invasões do governo ao domicílio.

> "O homem mais pobre pode em seu chalé desafiar todas as forças da Coroa. Pode ser frágil; seu telhado pode tremer; o vento pode soprar através dele; a tempestade pode entrar; a chuva pode entrar; mas o rei da Inglaterra não pode entrar - toda a sua força não ousa atravessar o limiar do cortiço arruinado!" William Pitt (1763 apud Henein, 2019, tradução nossa).

- 1890 - Os advogados americanos Samuel Warren e Louis Brandeis escreveram o direito à privacidade no artigo "*The Right to Privacy*", publicado na Harvard Law Review. Basicamente o artigo trata do direito de ser deixado em paz.
- 1948 - A partir da Declaração Universal dos Direitos Humanos, artigo 12, "ninguém será submetido a interferências arbitrárias em sua privacidade, família, lar ou correspondência, nem a ataques à sua honra e reputação. Todo mundo tem direito à proteção da lei contra tais interferências ou ataques."

- 1967 - Um novo marco foi alcançado com a publicação de "*Privacy and Freedom*", de Alan Westin, quando ele definiu a privacidade em termos de autodeterminação: privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles é comunicado aos outros.
- 1980 - A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define diretrizes sobre a proteção da privacidade e dos fluxos de dados pessoais entre os países.
- 1995 - A União Europeia cria a Diretiva de proteção de dados para regular o processamento de dados.
- 2002 - É criada pela União Europeia a Diretiva de Privacidade e Comunicações Eletrônicas.
- 2018 - No dia 25 de maio o GDPR passa a vigorar na União Europeia.
- 2018 - Poucos dias após a assinatura do GDPR, a China também publica um documento sobre proteção de dados, Padrão Nacional de Proteção de Informações Pessoais.
- 2018 - No dia 1 de junho é assinado o *California Consumer Privacy Act (CCPA) AB 375*, que surge no cenário americano, abrindo caminho para mudanças no cenário de privacidade dos EUA.
- 2018 - No dia 14 de agosto é assinada a Lei Geral de Proteção de Dados (LGPD) no Brasil.
- 2019 - Japão e União Europeia assinam no dia 13 de janeiro um acordo de adequação para facilitar os enlaces comerciais entre ambos.
- 2019 - No dia 15 de fevereiro é assinada na Tailândia a sua Lei de Proteção de Dados Pessoais.
- 2020 – No dia 18 de setembro entra em vigor no Brasil a Lei Geral de Proteção de Dados Pessoais.

2.2. Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (LGPD) vem de encontro a uma necessidade global referente à forma como dados pessoais são coletados e utilizados sem regulamentação alguma (DIVINO, 2019). Na prática, a LGPD foi criada como uma resposta às cobranças feitas pela União Europeia para que o Brasil tivesse uma legislação de mesmo nível de proteção (DANTAS BISNETO, 2020; IRAMINA, 2020).

O Regulamento Geral sobre a Proteção de Dados (GDPR), que trata do direito europeu sobre privacidade e proteção de dados pessoais, definiu e limitou de que forma deverá ocorrer o tratamento e processamento dos dados pessoais. Também regulamentou a exportação de dados pessoais para fora da União Europeia (UE) e Espaço Econômico Europeu (EEE) e tem como objetivo dar aos cidadãos e residentes formas de controlar os seus dados pessoais e unificar o quadro regulamentar europeu (FINKELSTEIN, 2019).

A LGPD, Lei 13.709, sancionada no dia 14 de agosto de 2018 é oriunda do PLC nº 4.060/12, que foi convertido no PLC nº 53/18. Além disso, altera a lei nº 12.965/16 (Marco Civil da Internet), e previa a entrada em vigor no dia 14 de agosto de 2020 com o principal objetivo de regulamentar o tratamento de dados pessoais, inclusive nos meios digitais, priorizando a sua privacidade (BRASIL, 2019). Em 8 de julho de 2019 foi incluída como emenda à Lei 13.853, complementando os conceitos e entendimentos da Lei 13.709. Para evitar sanções regulatórias e impulsionar o crescimento do cliente, as empresas que gerem dados devem adotar as melhores práticas para desenvolver e manter um programa eficaz de proteção de dados (PIURCOSKY *et at*., 2019).

Inspirada no Regulamento Geral sobre a Proteção de Dados da UE, a LGPD é uma regulamentação firmada em princípios. Ao determinar a proteção dos dados pessoais, busca garantir direitos aos cidadãos e estipula regras claras da forma como as operações de tratamento de dados realizados por órgãos públicos ou privados devem acontecer (DANTAS BISNETO, 2020). De acordo com Capanema (2020), para superar os desafios de controle que virão com a implantação da LGPD, será necessária uma mudança na forma de gerir os dados. Isso poderá evitar penalizações e multas desde a sua coleta até o seu armazenamento, visto que toda a cadeia de tratamento de dados é abordada na lei.

A LGPD é subdividida em dez capítulos com um total de 65 artigos que, similar ao GDPR, pretende esclarecer os principais conceitos envolvidos durante todo o processo de coleta, tratamento e armazenamento de dados pessoais. Os princípios fundamentais de tratamento são: finalidade, necessidade, transparência, prevenção, segurança, não discriminação, responsabilização e qualidade dos dados.

A LGPD afetará o processamento de todos os dados pessoais de pessoas residentes no Brasil. Por isso, desde a sua aprovação em agosto de 2018, as organizações públicas e privadas buscam estabelecer estratégias eficazes para atender as conformidades exigidas pela nova lei (NOVAKOSKI, NASPOLINI, 2020). O desafio é equilibrar a conformidade com a proteção da privacidade de clientes, funcionários, cidadãos, pacientes e consumidores para assim evitar a vulnerabilidade dos mesmos na exposição indevida de dados pessoais.

Basan e Faleiros Junior (2020) consideram que a avaliação de impacto na privacidade não é apenas uma tarefa necessária por meio da LGPD, mas um dever obrigatório para permitir que a seleção baseada em riscos de atividades e recursos atenda ao regulamento. Martini e Bergstein (2019) destacam que é importante lembrar que a discussão sobre privacidade no mercado brasileiro, baseada em conformidade regulatória, teve início com o Marco Civil da Internet (BRASIL, 2018). O tratamento de riscos de privacidade deve comparar os recursos necessários com as ofertas de fornecedores disponíveis. Também deve ser combinada as principais funções (como descoberta, mapeamento, classificação, controles de acesso e recursos em fim de vida), criando um ambiente de proteção e segurança dos dados (OLIVEIRA; ARAUJO, 2020).

Na visão de Leme e Blank (2020), a LGPD apresenta a segurança, prevenção e a adoção de medidas para o estabelecimento de boas práticas e governança no tratamento de dados pessoais como seus pilares. Nesse contexto destacam as três dimensões que direcionam os novos regulamentos de proteção de dados.

1. Legal, visto que a LGPD é uma lei e será aplicada a todos os dados pessoais.
2. Processual, pois dependendo do volume de negócios e dados, a conformidade com a LGPD pode exigir a implementação de (novas) funções, responsabilidades, responsáveis e processos.
3. Técnico, já que a LGPD inclui muitos princípios e requisitos de proteção de dados que devem ser avaliados pela tecnologia ou que exigem que a tecnologia limite o impacto nas operações internas.

Bedendo e Pegoraro Junior (2019) entendem que a privacidade está relacionada à confiança, ética e uma abordagem deliberada às atividades de processamento de dados pessoais. As leis informam a estratégia, a tecnologia permite um processamento intencional e o gerenciamento de riscos equilibra inovação com conservação. A proteção adequada da privacidade baseia-se no controle de dados pessoais durante todo o seu ciclo de vida (BARRETO JUNIOR, NASCIMENTO e FULLER, 2020), evitando assim a vulnerabilidade humana na exposição indevida dos dados. Para Oliveira *et al*. (2019), um aspecto essencial da LGPD é a mudança do paradigma da forma de coletar

dados para a captura apenas de dados que servem a um propósito deliberadamente iniciado e garantem controle e transparência nas atividades de processamento entre controladores e processadores de dados.

Assim como o GDPR, a LGPD estabelece que os titulares de dados têm direito a: aprovação de que seja realizado tratamento dos dados e que sejam anonimizados, acesso e retificação, bloqueio e descarte, anulação do consentimento, portabilidade, informação sobre os dados distribuídos, entendimento sobre a destinação, de não consentimento e ter ciência sobre o que pode acontecer, além da reavaliação de decisões automatizadas (DIVINO, 2019; TEFFÉ, 2020). A LGPD define os agentes de tratamento de dados e suas funções, buscando centralizar a fiscalização, regulamentar, efetivar a lei e decidir sobre os critérios da proteção de dados. Todas essas ações são gerenciadas pela Autoridade Nacional de Proteção de Dados (ANPD), criada pela medida provisória nº 869/18, (BRASIL, 2018). Quem administra bases de dados pessoais terá que fazer a gestão de riscos e falhas. Ocorrendo vazamento de dados, a ANPD e os cidadãos afetados devem ser avisados rapidamente. Falhas de segurança podem gerar multas pesadas para os responsáveis pelo tratamento de dados (BIONI; DIAS, 2020).

É importante frisar que a LGPD se aplica aos dados quando há interesse econômico. A LGPD não se aplica a pessoa natural para fins particulares e não econômicos. Também não se aplica para fins jornalísticos e artísticos, nesse caso impera a liberdade de expressão. Não se aplica para fins acadêmicos, ou seja, órgãos de pesquisa e instituições que realizam pesquisas estatísticas. Não é o mesmo que Educação a Distância e prestação de serviços educacionais, contudo, empresas que atuam no mercado da educação digital devem se adaptar a LGPD, obtendo, por exemplo, termos de uso e o consentimento do titular de dados.

A LGPD também não se aplica a Segurança Pública, Defesa Nacional, Segurança do Estado e até mesmo em casos de investigação e repressão penal. Também não se aplica ao processamento e ao tratamento de dados de fora do Brasil e que não seja objeto de comunicação. E nem ao uso compartilhado com agentes de tratamento do Brasil e ainda quando acontecer a transferência internacional de dados, desde que o país proporcione grau de proteção adequado ou equivalente àquilo que estabelece a LGPD.

Um fator muito importante que precisa ser levado em consideração ao tratar os dados é a segurança da informação. Piurcosky *et al*. (2019), destacam que a segurança da informação é fundamentada pelos conceitos de confidencialidade, integridade e disponibilidade. Por conta disso o sigilo designado à informação deve ser garantido. Para Oliveira e Araújo (2020) é necessário que existam mecanismos e ferramentas que possam garantir a segurança da informação, quando dados pessoais e dados sensíveis são utilizados no tratamento dos dados.

Para Agostinelli (2018), com a popularização da internet, a rede disponibiliza vários serviços digitais, onde as pessoas acabam utilizando dados pessoais, que muitas vezes ficam disponíveis para quem conseguir acessá-los. Para mitigar esse risco de exposição e, por conseguinte, a vulnerabilidade humana, a LGPD cria mecanismos que definem como esses dados devem ser armazenados e como podem ser compartilhados. Essas definições são importantes e devem estar relacionadas ao tipo de dado que transita por determinando meio.

Atualmente, está se presenciando um movimento até então inédito, a monetização dos dados pessoais, onde muitos serviços são pagos, integral ou parcialmente com os próprios dados pessoais do usuário. Segundo Lourenço e Taques (2020), a LGPD aparece como um meio irrefutável nos dias de hoje, ao conceder maior segurança jurídica à totalidade dos procedimentos que compreendem dados pessoais. A

regulação da proteção de dados pessoais tem que atuar, simultaneamente, como um mecanismo capaz de preservar e possibilitar atividades, além de habilitar os cidadãos e direcionar as ações dos agentes de mercado (GARCIA, 2020). Com a LGPD o Brasil está obtendo uma estrutura legal totalmente nova para proteção de dados que ultrapassa o alcance setorial, inclui todo o processamento e coleta de dados no território do país e pode muito bem chegar a uma decisão de adequação com o UE, uma vez que a LGPD é modelada de perto com o GDPR. De uma forma geral a LGPD cria um cenário de segurança jurídica válido para todo o país, com abrangência extraterritorial, pois não importa se a empresa ou o centro de dados estão no Brasil ou não. E permite o compartilhamento com outros países que também protejam dados.

O consentimento do titular de dados passa a ser a base para que dados possam ser tratados, sem ele, só se for indispensável para cumprir critérios legais (BARRETO JUNIOR, NASCIMENTO e FULLER, 2020). O consentimento no âmbito da LGPD é definido como um acordo explícito, inequívoco e concedido livremente por um titular de dados para permitir o processamento de seus dados pessoais. Para obter o consentimento, as organizações precisaram revisar suas aplicações. No entanto, segundo Finkelstein (2019), comparada com a obtenção de consentimento, manter evidências de consentimento poderá se tornar um desafio maior para as organizações. Para Leme e Blank (2020) é fundamental o consentimento qualificado do titular dos dados sensíveis para o seu tratamento, e também a utilização de sistemas digitais seguros como meios de proteger os direitos fundamentais da pessoa. A LGPD estabelece, de maneira clara, o que são dados pessoais, priorizando a finalidade e necessidade da sua utilização, quesitos de tratamento que devem ser previamente informados ao cidadão.

Para entender melhor a abrangência da LGPD é preciso definir seus principais conceitos, bem como destacar alguns pontos relacionados à proteção de dados pessoais e a privacidade do cidadão (BRASIL, 2018; BARRETO JUNIOR, NASCIMENTO e FULLER, 2020; GARCIA, 2020; MULHOLLAND, 2018; TEFFÉ e VIOLA, 2020):

- Titular dos dados: é a pessoa natural, pessoa física, identificada ou identificável, a quem aqueles dados se referem, portanto, de forma direta ou indireta que seja possível levar a identificação do seu titular. Empresas e startups, por exemplo, não estão abrangidos no escopo de proteção da LGPD, assim como as pessoas falecidas que não estão elencadas entre titulares de dados.
- Dados pessoais: são todas aquelas informações capazes de identificar o seu titular, por exemplo, nome, CPF, telefone, data e local de nascimento, e-mail, dados sobre contas em redes sociais etc.
- Dados pessoais sensíveis: são aqueles referentes às características da personalidade de uma pessoa, por exemplo, raça, etnia, convicção político-partidária, convicção religiosa, convicção filosófica, filiação sindical, dados de saúde, dados biométricos, até mesmo dados referentes à vida sexual de uma pessoa. Por esta razão merecem um tratamento especial por parte dos agentes de tratamento de dados. Dependendo do contexto, até mesmo selecionar um registro apontando para um indivíduo pode levar à identificação, como endereços IP, dados de localização, cookies ou número de registro de funcionário.
- Consentimento: manifestação livre, informada e inequívoca do titular de dados aceitando o tratamento de seus dados pessoais para uma finalidade determinada.

- Tratamento de dados: ações realizadas com o dado pessoal, por exemplo, coleta, classificação, utilização, reprodução, processamento, armazenamento e descarte.
- Agentes de Tratamento de Dados: controlador e processador, ambos podem ser uma pessoa física ou pessoa jurídica. Atuam diretamente no tratamento dos dados.
  - ✓ Controlador: detém o domínio das decisões, estabelece de que forma o tratamento será realizado e responde diretamente à autoridade supervisora. Muitas vezes ele contrata o processador.
  - ✓ Processador: realiza o tratamento dos dados de acordo com as normas definidas pelo controlador e somente da forma que ele determinar. Quando se entra na área de tecnologia da informação, existe a figura do subprocessador, que é aquele subcontratado ou terceirizado, para atuar de alguma forma no tratamento ou processamento dos dados pessoais. Nesse caso, o controlador deve ter total visibilidade das funções exercidas pelo subprocessador.
- Dados anonimizados: são aqueles em que é aplicada a técnica de anonimização, ou seja, é possível desvincular, desassociar o dado pessoal daquele titular. Duas formas muito comuns de aplicar essa técnica para se obter esses dados são:
  - ✓ Pseudonimização: um processo de anonimização onde se cria uma chave que pode ser usada para recuperar o identificador direto. Os dados pessoais e a chave são armazenados em um sistema seguro. Os dados confidenciais são armazenados em um sistema seguro, que criptografa os dados pessoais e retorna uma sequência alterada. A sequência do token pode ser usada posteriormente por uma parte autorizada para recuperar os dados originais.
  - ✓ Tokenização: também é um processo de anonimização de dados, é uma excelente estratégia para proteger dados. No entanto, à medida que o número de atributos de dados confidenciais aumenta e os dados se tornam mais distribuídos, o desempenho pode diminuir significativamente. Por esses motivos, é melhor limitar a tokenização a um atributo como endereço de e-mail. É bem possível gastar muito esforço para obter retorno mínimo ou dificultar a funcionalidade do sistema, se a tokenização não for tratada adequadamente.
- A Autoridade Nacional de Proteção de Dados (ANPD) é uma entidade criada pelo Poder Público Federal, vinculada à Presidência da República, que deve zelar pela proteção de dados. Tem competência para fiscalizar, aplicar sanções, definir normas, padrões e procedimentos, efetuar auditorias, estabelecer interpretações corretas de acordo com a LGPD. Cabe à ANPD fazer divulgação a respeito da educação, medidas para que todos estejam cientes dos seus direitos e proteções da lei e principalmente para que os controladores e processadores estejam devidamente adequados ao que determina a LGPD.

3. Metodologia

No que tange a natureza da pesquisa, os critérios de classificação dos tipos de pesquisa variam de autor para autor, obedecendo interesses, objetivos e campos. Ander-

Egg (1978) classifica em dois tipos: a pesquisa básica pura (BOOTH, COLOMB e WILLIAMS, 2019) ou fundamental, que é aquela que procura o progresso científico e tem por meta o conhecimento pelo conhecimento, e a pesquisa aplicada que, como o próprio nome já diz, tem interesses práticos na solução de problemas. A natureza desta pesquisa pode ser classificada como aplicada, já que visa analisar os aspectos a serem considerados por uma organização para se adequar à LGPD.

A estratégia para a coleta de informações foi a pesquisa bibliográfica, definida por Gil (2002) como um apanhado constituído, principalmente, por livros e artigos científicos. Sua proposta é analisar diferentes posições que englobam um determinado assunto. Marconi e Lakatos (2003) declaram ainda que essa pesquisa é elaborada a partir de importantes trabalhos realizados com capacidade de enriquecer o material a ser feito com dados atuais e relevantes.

Os artigos científicos foram coletados nas fontes Scielo, Google Acadêmico e Portal de Periódicos Capes (buscar assunto). A base de dados Scielo é uma biblioteca eletrônica que abrange uma coleção selecionada de periódicos científicos basicamente nos idiomas português e espanhol, com documentos revisados às cegas e por pares, atestando a sua qualidade. O Google Acadêmico é uma base de dados que reúne trabalhos oriundos da literatura acadêmica. No acervo, é possível encontrar artigos científicos, dissertações de mestrado, teses de doutorado, resumos, revistas de universidades e até mesmo livros. O Portal de Periódicos foi oficialmente criado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), e consiste de uma biblioteca virtual que reúne e disponibiliza um grande acervo científico de produção nacional e internacional.

O processo de pesquisa envolveu uma revisão sistemática da literatura por meio do protocolo PRISMA (MOHER *et al*., 2009), em quatro fases. Segundo Creswell (2010), a revisão de literatura oferece vários benefícios, por exemplo, fornece uma visão geral e abrangente das evidências disponíveis sobre um determinado tema de pesquisa. Além disso, ajuda a identificar lacunas de pesquisa no entendimento atual de um campo de estudo. Uma revisão da literatura pode destacar preocupações metodológicas em estudos de pesquisa que podem ser usados para aprimorar trabalhos futuros na área estudada. Por fim, podem ser usados para identificar questões para as quais as evidências disponíveis fornecem respostas claras e, portanto, para as quais pesquisas adicionais não são necessárias.

A revisão de literatura procura avaliar e comparar todas as evidências empíricas relevantes para fornecer uma interpretação completa dos resultados da pesquisa. Embora as revisões de literatura, em sua maioria, sejam normalmente usadas em pesquisa clínica e ciências sociais, elas encontraram aplicação em várias outras áreas, por exemplo, em publicidade, educação, desenvolvimento internacional, políticas públicas, ecologia, ciências ambientais, engenharia e pesquisa científica básica (MacKENZIE, 2012).

O processo de conduzir uma revisão de literatura, especialmente para novos autores, se mostra como um esforço valioso. Os autores refinam seus conhecimentos na área de interesse, desenvolvem novas ideias de pesquisa e adquirem habilidades críticas na síntese da literatura existente. Para Robson (2011), uma revisão sistemática da literatura é uma forma específica de identificar e sintetizar as evidências de uma ênfase em:

- Fornecer cobertura abrangente da literatura disponível no campo de interesse;
- Qualidade das evidências revisadas;
- Seguir uma abordagem detalhada e explícita para a síntese dos dados; e

- Utilização de processos transparentes e rigorosos ao longo da pesquisa.

A pesquisa buscou trazer publicações recentes de pelo menos cinco anos, em inglês e português, identificados até o mês de abril de 2021. Foram utilizadas na pesquisa as combinações de termos (LGPD OR "Lei Geral de Proteção de Dados").

4. Resultados e Análise

4.1. Revisão da Literatura

Baseada no protocolo PRISMA, a revisão sistemática da literatura identificou 3.758 registros, conforme mostrado no fluxo de informações (Tabela 1), seguidos de 64 na fase de seleção, 39 em elegibilidade, finalizando com 21 na fase de inclusão.

Tabela 1 – Fluxo de informações através das fases de uma revisão sistemática da literatura

Base Científica	Frases de Pesquisa	1. Identificação	2. Seleção	3. Elegibilidade	4. Inclusão
		Critérios de Exclusão =>	Título não alinhando com o escopo e Registros duplicados #3.694	Texto, método ou autor não disponível #26	Texto não alinhado com o escopo deste estudo #17
Scielo	(LGPD OR "Lei Geral de Proteção de Dados")	2	2	2	2
Portal Periódicos Capes		66	53	27	12
Google Acadêmico		3.690	10	10	7
	Total	3.758	64	39	21

Fonte: autores (2021).

Para a frase de pesquisa (LGPD OR "Lei Geral de Proteção de Dados"), foram identificados dois registros na base Scielo, 66 registros em periódicos revisados por pares no Portal de Periódicos Capes (buscar assunto), sendo que 26 não estavam disponíveis para acesso, e 3.690 registros no Google Acadêmico.

Os critérios de exclusão definidos foram: pesquisa em artigos científicos e aplicação da proteção de dados no contexto brasileiro (incluindo legislação e tecnologia).

Para obter dados significativos e com isso possibilitar a aplicação de mecanismos de busca nas bases científicas, foram identificados na primeira fase um total de 3.758 registros. Na segunda fase, foram excluídos 3.694 registros, selecionando um total de 64 registros para a terceira fase. Na terceira fase foram excluídos 26 registros, restando um total de 39 registros elegíveis para a quarta fase. Na quarta fase, foram excluídos 18 registros, totalizando 21 registros, que foram analisados e incluídos na fundamentação teórica.

4.2. Proposta conceitual

Na revisão da literatura foi possível observar que a LGPD é um tema interdisciplinar, que adentra a tecnologia utilizada, o processo de tratamento definido para lidar com os dados, o impacto de como a sua utilização afeta seus usuários, e os

direitos que cada cidadão tem em função de seus dados pessoais. A partir de uma análise do conteúdo dos estudos identificados e incluídos na fundamentação teórica, estabeleceu-se uma proposta conceitual dos aspectos relevantes a serem considerados por uma organização para se adequar à LGPD (Quadro 1).

Quadro 1 – Aspectos relevantes na adequação de uma organização à LGPD

Aspectos	Referências
Legislação	BASAN e FALEIROS JUNIOR (2020), BEDENDO e PEGORARO JUNIOR (2020), GARCIA (2020), IRAMINA (2020), LEME e BLANK (2020), TEFFÉ e VIOLA (2020).
Responsabilidade Civil	BIONI e DIAS (2020), CAPANEMA (2020), NOVAKOSKI e NASPOLINI (2020).
Segurança da Informação	OLIVEIRA *et al* (2019), PIURCOSKY *et at*. (2019).
Proteção de Dados e Privacidade	AGOSTINELLI (2018), FINKELSTEIN (2019), MARTINI e BERGSTEIN (2019), OLIVEIRA e ARAÚJO (2020).
Consentimento e Transparência	BARRETO JUNIOR, NASCIMENTO e FULLER (2020), LOURENÇO e TAQUES (2020), MULHOLLAND (2018), DANTAS BISNETO (2020), CARVALHO *et al*. (2019), DIVINO 2019).

Fonte: autores (2021).

O processo de criação de um programa de proteção de dados deve começar com um diagnóstico do estado atual da organização sobre o uso de dados pessoais em seus processos internos e externos e a criação de diretrizes que definam o melhor a metodologia utilizada. (ALLAN, 2019). Uma de suas diretrizes diz que os profissionais de segurança da informação e gerenciamento de riscos não podem agir sozinhos, mas devem envolver uma equipe multidisciplinar para traduzir requisitos e priorizar ações de mitigação de riscos.

Os profissionais de segurança da informação e gerenciamento de riscos devem definir um conjunto de controles de privacidade e segurança na adequação da regulamentação de privacidade. Nessa questão, a implementação de tecnologias pode ajudar a controlar e gerenciar dados pessoais, dando suporte à conformidade exigida na LGPD. Neiva e Willemsen (2019) destacam os cinco principais controles a serem criados: atribuir um encarregado de proteção de dados (DPO - *Data Protection Officer*), avaliar as lacunas, definir os períodos de retenção de dados, desenvolver a Governança de Dados e desenvolver um plano de resposta à violação de dados.

5. Considerações Finais

As novas leis de privacidade e proteção de dados exigem uma transformação fundamental na maneira como os dados pessoais são gerenciados. Devido à necessidade de manter a segurança desses dados, as novas leis se consolidaram de forma muito rápida nos últimos anos. A LGPD, por exemplo, busca dar mais garantias aos titulares de dados para assegurar que suas informações não sejam utilizadas de forma inadequada. Para atender esse princípio básico, muitas organizações precisam revisar seus processos de negócio.

Analisando o cenário atual, para tratar os riscos inerentes ao não cumprimento dos princípios da LGPD, as organizações devem cumprir algumas ações. Primeiro devem revisar suas políticas de segurança da informação incorporando os novos preceitos da LGPD. Depois devem reavaliar seus processos de negócio para identificar as melhores formas de atender o que é determinado pela LGPD. Além disso, as organizações devem verificar a necessidade de adequação tecnológica com o objetivo de suportar o aumento do volume de dados.

As organizações devem atender aos requisitos de conformidade de modo a agregar valor ao negócio, prezando pela privacidade do titular dos dados e adotando uma abordagem prática ao que a lei determina. Um conjunto bem definido e bem integrado de soluções tecnológicas pode fornecer às organizações a confiança necessária, disponibilizando um ambiente tecnológico capaz de proteger os dados pessoais que possuem.

Com base no contexto exposto, o objetivo deste trabalho foi identificar aspectos relevantes que devem ser considerados por uma organização para se adequar à LGPD, evitando assim a vulnerabilidade humana na exposição indevida dos dados pessoais. Considera-se que o objetivo foi atingido, a partir dos resultados apresentados. Como método de pesquisa, adotou-se uma revisão sistemática da literatura baseada no protocolo PRISMA, em quatro fases, envolvendo a identificação de registros nas bases Scielo, Portal de Periódicos CAPES (buscar assunto) e Google Acadêmico, e posteriormente a realização de uma seleção, verificação da elegibilidade e inclusão de 21 artigos na fundamentação teórica.

No Brasil, um grande problema enfrentado pelas organizações é justamente adequar seus processos e tecnologias para atender as demandas da LGPD. O desafio é proporcional à quantidade de dados manipulados, ao número de usuários e à complexidade do ambiente interno. A conformidade com a LGPD exigirá das organizações um planejamento estratégico cuidadoso, bem como escolhas ponderadas sobre as soluções tecnológicas necessárias.

Uma limitação deste estudo são as bases científicas pesquisadas, que não considerou bases de abrangência mundial como Scopus e Web of Science, mas isso não diminui a importância dos resultados encontrados, mais voltados à realidade brasileira, tratando da LGPD. A principal contribuição deste trabalho foi a elaboração de uma proposta conceitual sobre os aspectos relevantes a serem considerados por uma organização na adequação à LGPD, a saber: Legislação, Responsabilidade Civil, Segurança da Informação, Proteção de Dados e Privacidade, Consentimento e Transparência.

Para pesquisas futuras, é possível dar continuidade a este trabalho em algumas vertentes. A primeira é a realização de um estudo de caso em uma organização para verificar a aderência à proposta conceitual deste trabalho no que tange os aspectos a serem considerados na adequação à LGPD. A segunda é ampliar o campo de pesquisa abordando outros tipos de soluções tecnológicas não apontadas nesta pesquisa. A terceira é detalhar as arquiteturas de cada solução, aprofundando as suas especificidades.

Referências Bibliográficas

AGOSTINELLI, J. **A Importância da Lei Geral de Proteção de Dados Pessoais no Ambiente Online**. v. 14, n. 14 (2018) - ETIC 2018 - Encontro de Iniciação Científica - ISSN 21-76-8498.

ALLAN, A. **Hype Cycle for Identity and Access Management Technologies**. Gartner. 2019.

ANDER-EGG, E. **Introducción a las técnicas de investigación social: para trabajadores sociales**. 7. ed. Buenos Aires: Humanitas, 1978.

BARRETO JUNIOR, I. F.; NASCIMENTO, A. A. C.; FULLER, G. P. **Lei Geral de Proteção de Dados Pessoais - Efetividade Jurídica do Consentimento do Titular para Tratamento dos Registros**. Revista de Constitucionalização do Direito Brasileiro - RECONTO, v. 3, n. 2, 2020.

BASAN, A. P.; FALEIROS JUNIOR, J. L. M. **A proteção de dados pessoais e a concreção do direito ao sossego no mercado de consumo**. Revista eletrônica do Direito Civil. a. 9. n. 3, 2020.

BEDENDO, T. Z.; PEGORARO JUNIOR, P. R. **Lei Geral de Proteção de Dados Pessoais nas Relações do Comércio Eletrônico (Lei N. 13.709-2018)**. Univel. 2019.

BIONI, B.; DIAS, D. **Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. Revista Eletrônica do Direito Civil. a. 9, n. 3, 2020.

BOOTH, W. C.; COLOMB, G. G.; WILLIAMS, J. M. **A arte da pesquisa**. 3. ed. São Paulo: Martins Fontes, 2019.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 14 de agosto de 2018**. Presidência da República - Casa Civil - Subchefia para Assuntos Jurídicos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em 30 abr 2021.

CAPANEMA, W. A. A **responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, 2020.

CARVALHO, L.; OLIVEIRA, J.; CAPPELLI, C.; MAJER, V. **Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais**. In: Workshop de Transparência em Sistemas (WTRANS), Belém. Sociedade Brasileira de Computação. p. 21-30, 2019.

CRESWELL, J. C. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 3ª edição. Porto Alegre: Artmed, 2010.

DANTAS BISNETO, C. **Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado**. Revista Eletrônica do Direito Civil. v. 9, n. 3, 2020.

DIVINO, S. B. S. **Reflexões céticas, principiológicas e econômicas sobre o consentimento necessário à coleta e tratamento de dados**. Derecho PUCP, N° 83, 2019.

FINKELSTEIN, M. E.; FINKELSTEIN, C. **Privacidade e Lei Geral de Proteção de Dados Pessoais**. Revista de Direito Brasileira, Florianópolis, SC, v. 23, n. 9, p. 284-301, 2019.

GARCIA, R. C. de C. **Proteção de dados pessoais no Brasil: uma análise da Lei nº 13.709/2018 sob a perspectiva da Teoria da Regulação Responsiva**. Revista de Direito Setorial e Regulatório, Brasília, v. 6, nº 2, p. 45-58, 2020.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4ª edição. Editora Atlas, 2002.

HENEIN, N.; WILLEMSEN, B. **The State of Privacy and Personal Data Protection, 2019-2020**. Gartner Research. 2019. Disponível em: <https://www.gartner.com/doc/reprints?id=1-25UDD6NU&ct=210423&st=sb> Acesso em 16 jul 2021.

HOLVAST, J. **The Future of Identity in the Information Society**. Springer, Berlin, Heidelberg. 2008.

IRAMINA, A. **RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia**. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, nº 2, p. 91-117, 2020.

LEME, R. S.; BLANK, M. **Jurisprudência e legislação sanitária comentadas Lei Geral de Proteção de Dados e Segurança da Informação na área da Saúde**. Cadernos Ibero-americanos de Direito Sanitário, Brasília, 9(3), 2020.

LOURENÇO, A. L.; TAQUES, J. D. V. B. **O Papel das Ouvidorias Públicas na Implementação da Lei Geral de Proteção de Dados (LGPD)**. Revista do Ministério Público de Contas do Estado do Paraná. v. 7, n. 13, 2020.

LUKACS, A. **What is Privacy? The History and Definition of Privacy**. University of Szeged. 2016 Disponível em: <http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf>. Acesso em 16 jul 2021.

MacKENZIE, H. *et al*. **Systematic Reviews: What They Are, Why They Are Important, and How to Get Involved**. Journal of Clinical and Preventive Cardiology. 1(4):193-202. 2012.

MAGRANI, E. **A internet das coisas**. Rio de Janeiro. FGV Editora. 2018.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARTINI, S. R.; BERGSTEIN, L. **Aproximações entre o direito ao esquecimento e a Lei Geral de Proteção de Dados Pessoais (LGPD)**. Revista Científica Disruptiva. vol. 1, n. 1, 2019.

MOHER, D.; LIBERATI, A.; TETZLAFF, J.; ALTMAN, D. G.; THE PRISMA GROUP. **Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement**. PLoS Med, 6(7), 2009.

MULHOLLAND, C. S. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)**. Revista de Direitos e Garantias Fundamentais, 19(3), 159-180, 2018.

NEIVA, C.; WILLEMSEN, B. **Beyond GDPR: 5 Best Practices for LGPD Compliance**. Gartner. 2019.

NOVAKOSKI, A. L. M.; NASPOLINI, S. H. D. F. **Responsabilidade Civil na LGPD: Problemas e Soluções**. Conpedi Law Review. v. 6, n. 1, p. 158–174, 2020.

OLIVEIRA, A. C. S.; ARAÚJO, D. S. **O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados**. Liinc em Revista, Rio de Janeiro, v. 16, n. 2, e5318, 2020.

OLIVEIRA, N. S.; GOMES, M. A.; LOPES, R.; NOBRE, J. C. **Segurança da Informação para Internet das Coisas (IoT) - uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD)**. Revista Eletrônica de Iniciação Científica em Computação, v. 17, n. 4, 2019.

PIURCOSKY, F. P.; COSTA, M. A.; FROGERI, R. F.; CALEGARIO, L. L. **A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos**. SUMA DE NEGOCIOS, 10(23), 89-99, 2019.

POWER, E. **The Great Hack: The story of Cambridge Analytica, Trump and Brexit**. The Irish Time 2019.

ROBSON, C. **Real World Research: a resource for users of social research methods in applied settings**. 3rd Ed. West Sussex: John Wiley & Sons, Ltd., 2011.

SERPRO. **Empresas estão ou não preparadas para atender a LGPD?** 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/maioria-empresaainda-nao-estao-prontas-atender-lgpd/>. Acesso em 30 abr 2021.

TAKAHASHIA, A. R. W.; ARAUJO, L. **Case study research: opening up research opportunities**. RAUSP Manag. J. Vol. 55 No. 1, pp. 100-111. Emerald Publishing Limited. 2020.

TEFFÉ, C. S.; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Revista Eletrônica do Direito Civil. a. 9, n. 1, 2020.

UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia. Bélgica. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em 30 abr 2021.