UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

Um estudo sistemático sobre o impacto da adequação à *General Data Protection Regulation* (GDPR) pelas Organizações

Trabalho de Graduação

Aluno: Pedro Henrique Franco Machado
Orientadora: Jéssyka Flavyanne Ferreira Vilela
Área: Engenharia de Software

RECIFE
2022

Universidade Federal de Pernambuco
Centro de Informática

Pedro Henrique Franco Machado

Um estudo sistemático sobre o impacto da adequação à *General Data Protection Regulation* (GDPR) pelas Organizações

Trabalho de Conclusão de Curso apresentado no curso de Bacharelado em Engenharia da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.

Orientadora: *Jéssyka Flavyanne Ferreira Vilela*

RECIFE
2022

Este trabalho é dedicado à minha família, amigos e professores que sempre estiveram comigo e fizeram o melhor que podiam para me apoiar nos momentos em que mais precisei.

RESUMO

Contexto: a União Europeia foi pioneira na regulamentação do tratamento de dados pessoais ao implementar o Regulamento Geral sobre a Proteção de Dados, do inglês *General Data Protection Regulation* (GDPR). Entretanto, para atingir a conformidade com a lei GDPR, mudanças organizacionais precisam ser realizadas como, por exemplo, definir procedimentos de revisão, executar auditorias internas, elencar times responsáveis pelo cumprimento e formular políticas de atuação. **Objetivo:** compreender o impacto da adequação à GDPR pelas Organizações, analisando relatos de experiência, investigando o estado da arte, identificando as áreas afetadas e metodologias utilizadas. **Método:** a metodologia proposta para este trabalho foi uma Revisão Sistemática da Literatura. **Resultados:** após a execução da Revisão Sistemática da Literatura, foi possível compreender o impacto da adequação à GDPR pelas Organizações, identificando as áreas afetadas, os desafios encontrados e os métodos, tecnologias e práticas utilizadas. **Conclusões:** pode-se concluir que este trabalho contribuiu para o estado da arte e da prática com a obtenção de um panorama do processo de adequação e respectivo impacto gerado pela GDPR nas Organizações. A partir dessas informações, torna-se possível a identificação das áreas que sofreram um maior impacto com a legislação, dos desafios principais encontrados e o que foi mais utilizado como forma de mitigação para esses problemas identificados. Além disso, conseguiu-se identificar áreas que apresentaram problemas, mas ainda não encontraram nenhum tipo de solução para esses, o que pode estar evidenciando segmentos que precisam de uma maior atenção neste momento.

Palavras-chave: General Data Protection Regulation, GDPR, Impacto, Proteção de Dados.

ABSTRACT

Context: the European Union was a pioneer in regulating the processing of personal data with the implementation of the General Data Protection Regulation (GDPR). However, to achieve GDPR compliance, organizational changes must be made, such as, defining review procedures, performing internal audits, listing teams responsible for compliance and formulating action policies. **Objective:** understand the impact of GDPR compliance by Organizations, analyzing experience reports, investigating the state of the art, identifying the affected areas and methodologies used. **Method:** the methodology proposed for this work was a systematic literature review. **Results:** after carrying out a systematic literature review, it was possible to understand the impact of compliance with GDPR by Organizations, identifying the affected areas, the challenges encountered and the methods, technologies and practices used. **Conclusion:** it can be concluded that this work contributed to the state of the art and practice by obtaining an overview of the adaptation process and the respective impact generated by GDPR on Organizations. From this information, it becomes possible to identify the areas that suffered the greatest impact with the legislation, the main challenges encountered and what was most used as a way of mitigating these identified problems. In addition, it was possible to identify areas that presented problems, but have not yet found any kind of solution for them, which may be showing segments that need greater attention at this time.

Keywords: General Data Protection Regulation, GDPR, Impact, Data Protection.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. Introdução

1.1. Contexto

O nascimento da Internet remonta ao final dos anos 60, financiado pelo departamento de defesa dos EUA com o *Advanced Research Projects Agency Network* (ARPANET) [38]. Desde então, a tecnologia se desenvolveu até a invenção da *World Wide Web* (WWW) nos anos 90, marco para que se chegasse na rede mundialmente conectada que é conhecida hoje. Desde 2000, a Internet cresceu mais de 1300% [39]. Em 2021, existiam mais de 5,16 bilhões de usuários ativos, o que representa mais de 65% da população mundial [39].

Nos dias atuais, vive-se a quarta revolução industrial, onde comunicações móveis, redes sociais e sensores estão encurtando os limites entre pessoas, a Internet e o mundo físico [40]. Essa nova revolução é precedida pela economia digital, onde mercados deixam espaço para redes e acesso constitui uma propriedade [41].

Tecnologias digitais permitem o estudo de bilhões de trocas individuais, em que pessoas diariamente fazem transações de ideias, dinheiro, bens e comunicações [42]. A Internet, telefones celulares, sensores integrados e outros dispositivos eletrônicos geram dados diariamente [43].

Nas últimas décadas, os avanços tecnológicos acarretaram em um grande aumento na escala e na precisão dos dados pessoais que são coletados por instituições. Tal progresso foi acompanhado por avanços na área de *Machine Learning* e tecnologias de processamento de informações, que permitiram a essas instituições transformar os dados coletados em produtos e serviços de sucesso com grandes retornos econômicos. Caracterizado como “o novo petróleo" e “uma nova classe de bens” [44], informações pessoais são o epicentro da economia digital.

Em contrapartida, existe um crescimento no número de casos de vazamentos de dados, como a British Airways, companhia aérea britânica, que foi multada em cerca de 20 milhões de libras por vazar informações pessoais e de pagamento de mais de 400 mil clientes em 2018 [51] e do Marriott Internacional, empresa dona de um conglomerado de hotéis de luxo, que foi multada em 18,4 milhões de libras por um vazamento de 339 milhões de registros sobre hóspedes em 2014 [52]. Com tais casos, também aumenta o desânimo entre usuários em relação ao seu pouco controle nesse processo. A respeito disso, reguladores governamentais têm proposto e promulgado legislações sobre a privacidade de dados, que empoderam os usuários no sentido de ter mais autoridade sobre as informações que geram.

A União Europeia foi pioneira na implementação de uma regulamentação desse tipo, entrando em vigor em Maio de 2018 a *General Data Protection Regulation* (GDPR) [45]. A GDPR estabelece regras para o processamento, proteção, armazenamento e utilização de informações pessoais. Em seu discurso na conferência do Regulamento Geral de Proteção de Dados, a Comissária de Valores e Transparência, Věra Jourová, afirma: “*Não é o final do caminho, mas sim o começo de um novo capítulo*” [53]. Tal lei, serviu como base para legislações sobre privacidade em diversos países, como o Brasil, Chile, Nova Zelândia, Índia, e estados americanos, como a Califórnia [46].

1.2. Motivação e Justificativa

Organizações lidam com constantes mudanças sobre normas legais e regulamentais. Nesse contexto, para que se mantenham em conformidade, as Organizações precisam efetuar mudanças organizacionais como, por exemplo, definir procedimentos de revisão, executar auditorias internas [54], elencar times responsáveis pelo cumprimento e formular políticas de atuação [55].

A GDPR tem sido objeto de estudo por vários trabalhos na literatura [56][57][58]. Por exemplo, em 2019, Teixeira, Silva e Pereira realizaram um trabalho com o objetivo de identificar os fatores críticos de sucesso da implementação da GDPR [56]. Em 2018, Kutz, Semmann e Böhmann fizeram uma revisão sobre *Privacy by Design* (PbD), focando em trabalhos que buscam a implementação de PbD em organizações, localizadas em ecossistemas [57]. Em 2021, Bassani e Cazella conduziram um estudo que buscou identificar pesquisas acadêmicas relacionadas à temática de Análise de Aprendizagem, do inglês *Learning Analytics* (LA), que consiste na utilização de dados de aprendizagem para fazer análises sobre o desempenho educacional de estudantes, e GDPR [58].

Entretanto, não foi encontrado um estudo que reúna evidências sobre o impacto nas Organizações sobre o processo de adequação à GDPR. Portanto, constata-se uma lacuna sobre o impacto e as mudanças que têm ocorrido nas Organizações para atingir a conformidade com a lei. Sendo assim, este trabalho se propõe a investigar tais impactos.

1.3. Objetivos

Nesse contexto, este trabalho tem como objetivo compreender o impacto da adequação à GDPR pelas Organizações.

Para atingir este objetivo geral, os seguintes objetivos específicos foram definidos:

- Analisar relatos de experiência das Organizações;
- Investigar o estado da arte e as práticas adotadas pelas Organizações para atingir conformidade com a GDPR;
- Identificar as áreas afetadas e metodologias usadas no processo de adequação a GDPR.

O método de pesquisa a ser utilizado para satisfazer os objetivos é uma Revisão Sistemática da Literatura a ser descrita na Seção 3.

1.4. Trabalhos Relacionados

Atualmente, a lei GDPR tem sido foco de estudo de diversos trabalhos na literatura [56][57][58]. Em 2019, Teixeira, Silva e Pereira [56] realizaram uma Revisão Sistemática da Literatura (RSL) com o objetivo de identificar os fatores críticos de sucesso da implementação da GDPR, obtendo sucesso no mapeamento de tais fatores, incluindo barreiras e facilitadores, além de identificar os benefícios da adequação à GDPR [56].

Em 2018, Kutz, Semmann e Böhmann [57] conduziram uma RSL sobre PbD, com foco em publicações que buscavam a implementação de PbD em Organizações localizadas

em ecossistemas. Os resultados mostraram uma surpreendente escassez de pesquisas nesse campo, mesmo com a ênfase da lei nessa questão crítica [57].

Em 2021, Bassani e Cazella realizaram uma RSL com o propósito de identificar pesquisas acadêmicas relacionadas à temática de LA e GDPR, cuja análise possibilitou concluir que há um alinhamento entre esses conceitos e que a LA deve seguir as orientações da GDPR [58].

A Tabela 1.1 apresenta as principais semelhanças e diferenças entre este trabalho e os principais trabalhos relacionados.

Tabela 1.1 - Comparação entre trabalhos relacionados e o trabalho proposto.

Critério	**Kutz C, Semmann M, Böhmann T. (2018)**	**Teixeira G, Mira da Silva M e Pereira, R. (2019)**	**Bassani R, Cazella S. (2021)**	**Trabalho Proposto**
Lei de privacidade contemplada	GDPR	GDPR	GDPR	GDPR
Tipo de contribuição	Revisão Sistemática da Literatura.	Revisão Sistemática da Literatura.	Revisão Sistemática da Literatura.	Revisão Sistemática da Literatura.
Objetivo	Investigar trabalhos que buscaram a implementação de *Privacy by Design* (PbD) em organizações, localizadas em ecossistemas.	Identificar os fatores críticos de sucesso da implementação da GDPR e identificar os benefícios da adequação à lei.	Identificar pesquisas acadêmicas relacionadas à temática *Learning Analytics* (LA) e GDPR.	Compreender o impacto da adequação à GDPR pelas Organizações, analisando relatos de experiência, investigando o estado da arte, identificando as áreas afetadas e metodologias utilizadas.
Quantidade de trabalhos selecionados na Revisão Sistemática	39	32	10	37
Resultados	Os resultados mostram uma escassez de pesquisas neste campo, embora a GDPR enfatize explicitamente essa questão crítica.	Os fatores críticos de sucesso da implementação do GDPR foram identificados, incluindo barreiras e facilitadores. Além disso, também foram identificados os benefícios do cumprimento da GDPR.	Após a aplicação dos critérios de inclusão e exclusão sobre os artigos obtidos, foram selecionados dez textos, cuja análise possibilitou concluir que há um alinhamento entre os conceitos de LA e GDPR e que a LA deve seguir as orientações da	Após a execução da Revisão Sistemática da Literatura, foi possível compreender o impacto da adequação à GDPR pelas Organizações, identificando áreas afetadas, desafios encontrados e métodos,

			GDPR.	tecnologias e práticas utilizadas.

Fonte: O autor.

Analisando os trabalhos apresentados na Tabela 1.1, observa-se que o estudo realizado por Teixeira, Silva e Pereira [56] identificou os fatores de sucesso, barreiras, facilitadores e benefícios da adequação à GDPR. Este trabalho contribui com a identificação das áreas afetadas e soluções aplicadas pelas Organizações para atingir a conformidade com a GDPR. A RSL conduzida por Kutz, Semmann e Böhmann [57] aponta que poucos dos trabalhos analizados abordam explicitamente terceiros e suas integrações nas práticas da Organizações para adequação ao processamento de dados determinado pela GDPR, para lidar com essa deficiência, o trabalho propõe um guia de pesquisa que capacita e orienta sobre esse processo. A publicação feita por Bassani e Cazella [58] conclui que existe um alinhamento entre os conceitos de LA, uma área que se propõe a medir, coletar, analisar e relatar dados de discentes em seus contextos, o que traz à tona uma nova preocupação, relacionada à proteção, à privacidade e ao correto uso desses dados, e GDPR. Tal estudo, identificou, inicialmente, que a ética vem influenciando os construtores de sistema de LA desde a concepção e que o Learning Analytics abre um cenário complexo de questões de privacidade e políticas, que, por sua vez, influenciam como os sistemas e práticas de análise de aprendizado são e serão projetados, também foi observado que os desenvolvedores de LA estão seguindo as orientações definidas pela legislação europeia. Este trabalho complementa os trabalhos relacionados ao avaliar os impactos causados pela adequação à legislação por parte das Organizações, em função das áreas afetadas, desafios e técnicas utilizadas.

1.5. Estrutura do Documento

Este documento está estruturado da seguinte forma: na Seção 2 são apresentados os principais conceitos envolvidos nesse trabalho; na Seção 3 é descrita a metodologia de pesquisa adotada neste trabalho; na Seção 4 são apresentados os resultadas encontrados; e, finalmente, na Seção 5 são discutidas as conclusões e trabalhos futuros.

2. Revisão de Literatura

Nesta seção, são descritos os principais conceitos envolvidos neste trabalho.

2.1. Leis de Privacidade

O conceito de Lei de Privacidade se refere a todas as leis aplicáveis no mundo que tem relação com o processamento, privacidade e segurança de dados pessoais e, além disso, a todos os regulamentos emitidos sob esse mesmo contexto [61], como é o caso da GDPR, da legislação brasileira: Lei Geral de Proteção de Dados Pessoais (LGPD) e do regulamento aplicado na Califórnia: *California Consumer Privacy Act* (CCPA).

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural [62]. Existem vários pontos de convergência entre o regulamento europeu e a lei brasileira. Dentre esses, podem ser destacados: o conceito de dado pessoal, a ideia principal de direito à proteção dos dados pessoais, o território de abrangência dos normativos que não se restringem apenas ao território europeu, no caso do GDPR, ou ao território brasileiro, no caso da LGPD, o conceito de responsável pelo tratamento ou controlador, o conceito do processo de pseudonimização, as hipóteses previstas para a transferência de dados internacionalmente e a função da Autoridade Nacional [65].

A CCPA oferece aos consumidores mais controle sobre as informações pessoais que as empresas coletam sobre eles e fornece orientações sobre como implementar a lei [63]. Esse regulamento passou a garantir novos direitos de privacidade para os consumidores da Califórnia, como, por exemplo, o direito de saber sobre as informações pessoais que uma empresa coleta sobre elas e como elas são usadas e compartilhadas. Embora pareça próxima aos conceitos da GDPR, os dois regulamentos diferem em alguns aspectos. O regulamento europeu se aplica a controladores e processadores de dados, enquanto a CCPA se aplica a empresas com fins lucrativos que atendem a residentes da Califórnia [64]. Isso significa que a GDPR é muito mais ampla, tanto para os cidadãos que protege quanto para as organizações às quais se aplica.

2.2. GDPR

Atualmente, a sociedade está cada vez mais se beneficiando, de forma significativa, da crescente digitalização e conectividade que a Internet proporciona, tornando mais eficiente o modo como as pessoas se comunicam, interagem e trabalham.

No entanto, essa crescente dependência tecnológica também traz novas formas de vulnerabilidades, riscos e exposição para os cidadãos, economias e administrações [36], tornando-se necessária a aplicação de direitos sobre a proteção de dados pessoais.

A legislação européia, *General Data Protection Regulation* (GDPR), estabelece regras relativas à proteção das pessoas naturais no que diz respeito ao tratamento de dados pessoais e regras relativas à livre circulação de dados pessoais [45], protege os direitos e liberdades fundamentais das pessoas naturais e, em particular, o seu direito à proteção dos dados pessoais. A GDPR está sendo implementada para padronizar e modernizar as leis de proteção de dados relacionadas à Internet, redes sociais e mercados digitais [36].

A lei foi aprovada em 14 de abril de 2016 e está em vigor desde 25 de maio de 2018. Ao contrário da diretiva de proteção de dados, do inglês *Data Protection Directive,* 95/46/EC, onde os países membros da União Europeia decidiram a natureza de sua implementação, a GDPR é um regulamento aprovado pelo parlamento europeu e, portanto, vinculativa à todos os países membros, substituindo as leis nacionais [19].

A lei é composta por 99 artigos que descrevem seus requerimentos legais e 173 recitais que fornecem contexto adicional e clarificação para esses artigos. Tais artigos podem ser agrupados em 5 categorias: artigos 1-11 explicam sobre as definições e princípios do

processamento de dados pessoais, artigos 12-23 estabelecem os direitos das pessoas, artigos 24-50 esclarecem as responsabilidades dos controladores e operadores de dados, por fim, os últimos 26 artigos explicam o papel e tarefas das autoridades, multas e situações específicas [17].

Das novas de funções estabelecidas que lidam com assuntos relacionados à proteção de dados pessoais, podem ser mencionadas [36]:

- ***Data controller*** **(controlador de dados):** pessoa física ou jurídica, autoridade, ou órgão que, sozinho ou em conjunto com outros, determina a finalidade e os meios de tratamento de dados pessoais. Definir medidas técnicas e organizacionais para garantir e demonstrar que o processamento de dados é realizado de acordo com a GDPR é papel do controlador de dados;
- ***Data processor*** **(processador de dados):** pessoa jurídica natural, autoridade ou organização que manipula dados pessoais em nome do controlador. Esses precisam atender aos padrões estabelecidos pelos controladores com as garantias suficientes;
- ***Data protection officer*** **- DPO - (responsável pela proteção de dados):** função designada pelo controlador e operador dos dados cuja responsabilidade é supervisionar a estratégia e implementação de proteção de dados de uma organização, para garantir que ela esteja em conformidade com os requisitos da GDPR;

São garantidos pela GDPR os seguintes princípios relacionados ao processamento de dados pessoais [45][59]:

- **Princípio da licitude, lealdade e transparência (l*awfulness, fairness and transparency*):** estabelece que o processamento de dados pessoais deve ter uma justificativa legal para acontecer, além da transparência do motivo apresentado;
- **Princípio da limitação de finalidade (*purpose limitation*):** a coleta de dados pessoais deve ter fins específicos, explícitos e legítimos;
- **Princípio da minimização de dados (*data minimisation*):** a coleta de dados pessoais deve estar limitada apenas ao necessário para aquilo que se destina seu uso;
- **Princípio da exatidão (*accuracy*):** dados precisos e só utilizados quando necessário;
- **Princípio de limitação de armazenamento (*storage limitation*):** o formato dos dados pessoais deve permitir a identificação apenas do necessário a ser utilizado;
- **Princípio de integridade e confidencialidade (*integrity and confidentiality*):** o processamento dos dados pessoais deve garantir a segurança dos mesmos;
- **Princípio da responsabilização (*accountability*):** o responsável pelo uso dos dados deve cumprir rigorosamente os princípios.;

Tais princípios, estão ilustrados na Figura 2.1.

Figura 2.1 - Princípios relacionados ao processamento de dados pessoais

Fonte: O autor.

Dos novos direitos relacionados a proteção de dados pessoais em Organizações, podem ser mencionados [36]:

- **Acessar informações sobre dados pessoais:** o indivíduo tem o direito de obter dados dos controladores sobre seu tratamento de dados pessoais e, quando for o caso, o acesso a esses dados pessoais e a obtenção de informações sobre, entre outras coisas, a finalidade do tratamento, as categorias de dados pessoais e os terceiros a quem dados pessoais foram divulgados;
- ***Right to be forgotten*** **(Direito a ser esquecido):** um titular de dados tem o direito de obter a exclusão dos dados pessoais que lhe digam respeito sem demora injustificada;
- **Tomada de decisão individual automatizada:** o titular dos dados tem o direito de não estar sujeito a uma decisão baseada no processamento automatizado de dados;
- **Consentimento:** os dados pessoais não podem ser processados sem consentimento, a menos que expressamente permitido por lei;
- **Limite de tempo:** os dados pessoais não devem ser mantidos por um tempo maior do que o necessário para os fins que foram processados, mas podem ser armazenados por períodos mais longos no caso de interesse público ou pesquisas com propósito histórico e científico.

A conformidade com a GDPR é um veículo para trazer melhorias no fluxo de dados, otimizar as atividades do dia-a-dia e gerar mais valor para clientes e stakeholders [36]. Observa-se que, mesmo com pouco tempo de existência, o regulamento se tornou referência para legislações referentes à privacidade de dados. Países como Rússia, Brasil, Índia e Japão

estão seguindo seu exemplo para criar regulamentos que padronizem a proteção de dados pessoais [19].

3. Metodologia

A metodologia proposta para este trabalho foi uma Revisão Sistemática da Literatura (RSL). Esse método de pesquisa trata-se de um meio para identificar, avaliar e interpretar estudos relevantes para uma determinada pergunta de pesquisa, área ou fenômeno de interesse [47].

Inicialmente, foi realizada uma revisão não sistemática da literatura, que consistiu em uma pesquisa sobre trabalhos relacionados ou que tenham conceitos em comum com a temática de interesse. Após esse estudo inicial, foi conduzida a RSL seguindo as três principais fases sugeridas por Kitchenham e Charters [47]: Planejar a revisão, conduzir a revisão e reportar a revisão.

Os estágios associados a planejar a revisão são:

- Identificar a necessidade para a revisão;
- Comissionar a revisão;
- Especificar a(s) pergunta(s) de pesquisa;
- Desenvolver um protocolo de revisão;
- Avaliar o protocolo de revisão;

Os estágios associados a conduzir a revisão são:

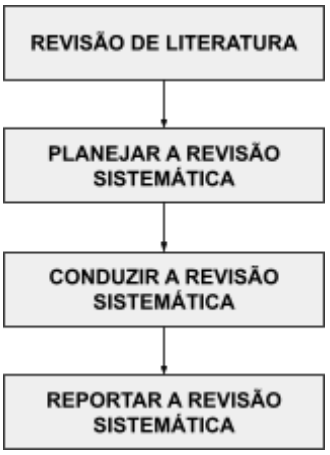
- Identificação da pesquisa;
- Seleção de estudos primários;
- Avaliar a qualidade dos estudos;
- Extração de dados e monitoramento;
- Síntese dos dados;

Os estágios associados a reportar a revisão são:

- Especificar os mecanismos de divulgação;
- Formatar o relatório principal;
- Avaliar o relatório;

Os passos da metodologia de pesquisa para alcançar os objetivos descritos na Seção 1.3 estão ilustrados na Figura 3.1.

Figura 3.1 - Metodologia de pesquisa



Fonte: O autor.

O protocolo de revisão, que foi definido utilizando o Parsifal (https://parsif.al/), ferramenta online projetada para apoiar pesquisadores a realizar RSL no contexto da Engenharia de *Software*, será detalhado nas próximas seções.

3.1. Questões de Pesquisa

Este trabalho tem como objetivo compreender o impacto da adequação à GDPR pelas Organizações. Para isso, por meio de uma RSL proposta por Kitchenham e Charters (2007) [47], pretende-se responder uma questão de pesquisa, apresentada na Tabela 3.1.

O protocolo de revisão proposto utilizou os critérios PICOC (População, Intervenção, Comparação, Resultados e Contexto) [47] para formulação das perguntas de pesquisa. Neste trabalho, os critérios foram definidos da seguinte forma:

- **População:** Estudos empíricos que abordam o impacto da GDPR nas Organizações do mundo;
- **Intervenção:** Coletar evidências empíricas para responder às perguntas de pesquisa;
- **Comparação:** Não se aplica;
- **Resultados:** Respostas para as perguntas de pesquisa;
- **Contexto:** Qualquer contexto que aborde os desafios e métodos/tecnologias/práticas nas Organizações do mundo em virtude da implementação da GDPR;

Tabela 3.1 - Questão de pesquisa

Identificador	Questão de Pesquisa
P1	De acordo com a literatura, qual é o impacto gerado pela GDPR nas Organizações do mundo?

Fonte: O autor.

A pergunta P1 será respondida por meio de uma análise sobre os resultados das subperguntas P1.1, P1.2 e P1.3, apresentadas na Tabela 3.2.

Tabela 3.2 - Subperguntas de pesquisa

Identificador	Subpergunta de Pesquisa
P1.1	De acordo com a literatura, quais são as áreas afetadas com a adequação a GDPR?
P1.2	De acordo com a literatura, quais são os desafios que as Organizações encontraram para e com a adequação a GDPR?
P1.3	De acordo com a literatura, quais são os métodos/tecnologias/práticas que as Organizações utilizam para a adequação a GDPR?

Fonte: O autor.

Respondendo tais perguntas, será possível compreender o impacto da adequação à GDPR pelas Organizações e, assim, identificar áreas afetadas, desafios encontrados e métodos/tecnologias/práticas utilizadas.

3.2. Estratégia de Busca

A estratégia de busca utilizada neste trabalho seguiu os passos de Kitchenham e Charters (2007) [47]. Inicialmente, foram levantadas palavras-chave e sinônimos, conforme mostrado na Tabela 3.3.

Tabela 3.3 - Palavras-chave e sinônimos

Palavras-chave	Sinônimos
GDPR	-
General Data Protection Regulation	-
Impact	Consequence, Effect, Influence, Result.

Fonte: O autor.

Além das palavras-chave, previamente, foram selecionados 4 estudos de controle como forma de validação da completude dos resultados apresentados pela string de busca. Esses estudos estão listados na Tabela 3.4 e foram selecionados por pertencerem ao escopo desse trabalho.

Tabela 3.4 - Estudos validadores

Estudo de controle	Citação
An Empirical Study on the Impact of GDPR and Right to Be Forgotten - Organizations and Users Perspective	[18]
GDPR Impact on Computational Intelligence Research	[4]
Towards privacy compliance: A design science study in a small organization	[21]
General Data Protection Regulation in Health Clinics	[30]

Fonte: O autor.

As buscas pelos artigos foram realizadas nas bases listadas na Tabela 3.5.

Tabela 3.5 - Bases de busca

Nome	**URL**
ACM Digital Library	http://portal.acm.org
IEEE Digital Library	http://ieeexplore.ieee.org
Science@Direct	http://www.sciencedirect.com
Springer Link	http://link.springer.com

Fonte: O autor.

Considerando o objetivo desta RSL, as palavras-chave e os estudos de controle, definiu-se a seguinte string de busca:

("GDPR" OR "General Data Protection Regulation") AND ("Impact" OR "Consequence" OR "Effect" OR "Influence" OR "Result")

3.3. Critérios de Seleção

Os critérios de inclusão e exclusão utilizados neste trabalho são apresentados, respectivamente, na Tabela 3.6 e Tabela 3.7.

Tabela 3.6 - Critérios de inclusão

Identificador	**Critérios de Inclusão**
CI1	Apenas artigos completos (full papers) foram aceitos.
CI2	O estudo deve ser único. Quando diferentes artigos são escritos pelos mesmos autores descrevendo os mesmos assuntos com pequenas modificações, foi escolhido o mais completo, mais atual e abrangente.
CI3	Os estudos devem estar diretamente relacionados à GDPR e sua implementação no mundo.
CI4	Foram aceitos apenas artigos escritos em Inglês ou Português.

Fonte: O autor.

Tabela 3.7 - Critérios de exclusão

Identificador	**Critérios de Exclusão**
CE1	Estudos com data de publicação inferior a 2018 foram excluídos (i.e., apenas estudos entre 2018 - 2022 serão considerados).
CE2	Estudos no contexto da GDPR, mas focados apenas no campo teórico do Direito foram excluídos.

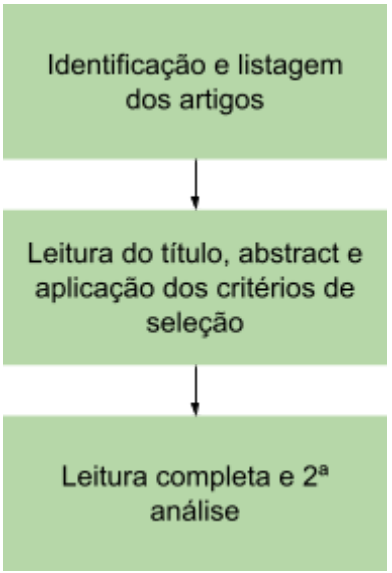
CE3	Estudos que apresentem apenas opiniões sem qualquer evidência empírica de apoio foram excluídos.
CE4	Estudos que não focavam no contexto GDPR foram excluídos.
CE5	Estudos que não puderam ser encontrados facilmente na forma de texto completo em bibliotecas digitais conhecidas (e.g., IEEE, Scopus, Science Direct, ACM and etc) foram excluídos.
CE6	Estudos relacionados à privacidade de dados em geral, mas que não levam em consideração a GDPR foram excluídos.
CE7	Estudos repetidos foram excluídos.

Fonte: O autor.

3.4. Procedimento para a Seleção de Estudos

O procedimento de seleção dos estudos foi realizado em 3 etapas. Primeiramente, foram identificados e listados todos os artigos que retornaram como resultado após a aplicação da string de busca nas bases. Em seguida, foi realizada a leitura do título, abstract e aplicação dos critérios de inclusão e exclusão. Por fim, foi realizada a leitura completa dos artigos selecionados compreendendo uma 2ª análise, a fim de identificar se o artigo respondia alguma das subperguntas de pesquisa definidas na Seção 2.1. O procedimento está ilustrado na Figura 3.2.

Figura 3.2 - Procedimento de seleção de estudos



Fonte: O autor.

3.5. Avaliação de Qualidade

De acordo com Kitchenham e Charters (2007) [47], a qualidade de um artigo se relaciona com a extensão em que o estudo minimiza o viés e maximiza a validade interna e externa.

Nesta RSL, foi utilizada uma técnica de pontuação para avaliar a credibilidade, integridade e relevância dos estudos selecionados. Todos os artigos foram avaliados com base em 5 perguntas, listadas na Tabela 3.8.

Tabela 3.8 - Perguntas de qualidade

Identificador	Pergunta de Qualidade
PQ1	O estudo traz considerações sobre suas limitações ou ameaças à validade?
PQ2	O estudo define os objetivos ou questões de pesquisa de forma clara?
PQ3	O estudo faz uma clara descrição do contexto na qual a pesquisa foi realizada?
PQ4	Os resultados encontrados estão dispostos de forma clara?
PQ5	O estudo faz uma análise/discussão sobre os dados apresentados?

Fonte: O autor.

Cada pergunta foi julgada em três opções de resposta possíveis: opção 1, significa que o estudo cumpriu o critério completamente e tem pontuação 1,00, opção 2, significa que o estudo cumpriu o critério parcialmente e tem pontuação 0,50 e opção 3, significa que o estudo não cumpriu o critério e tem pontuação 0,00.

A pontuação final de um artigo é calculada pela soma da pontuação de cada resposta. Caso a pontuação do artigo seja maior que 2,50, o trabalho foi selecionado para extração de dados para responder às perguntas de pesquisa.

3.6. Extração dos Dados

Através da ferramenta Parsifal, um formulário de extração de dados foi definido. Neste, foram registradas as informações referentes ao artigo e o que era relevante para as subperguntas de pesquisa. Na Tabela 3.9 são apresentados os campos presentes no formulário.

Tabela 3.9 - Campos presentes no formulário de extração de dados

Campo	Tipo de dado
ID	Número
TÍTULO	Texto
AUTORES	Texto
METODOLOGIA	Texto
CONFERÊNCIA/LOCAL DE PUBLICAÇÃO	Texto
ANO	Número
TIPO DO ESTUDO	Texto

P1.1: De acordo com a literatura, quais são as áreas afetadas com a adequação da GDPR?	Texto
P1.2: De acordo com a literatura, quais são os desafios que as Organizações encontraram para e com a adequação da GDPR?	Texto
P1.3: De acordo com a literatura, quais são os métodos/tecnologias/práticas que as Organizações utilizam para a adequação da GDPR?	Texto
COMENTÁRIOS ADICIONAIS/CONSIDERAÇÕES	Texto

Fonte: O autor.

3.7. Ameaças à validade

Neste trabalho, utilizou-se a classificação de ameaças à validade descrita por Wohlin [60]. Tal classificação define 4 tipos de ameaças de validade, sendo essas, ameaças de conclusão, internas, construção e externas.

Conclusão: envolve avaliar em quão certos podemos estar de que o tratamento que usamos em um experimento realmente está relacionado ao resultado real que observamos. Para amenizar os efeitos dessa ameaça, o processo da revisão foi cuidadosamente elaborado e discutido pelo aluno e orientadora a fim de minimizar o risco de exclusão de estudos relevantes.

Internas: aborda o quão certos podemos estar de que o tratamento realmente causou o resultado. Podem haver outros fatores que causaram o resultado, fatores que não temos controle sobre ou não medimos. A fim de minimizar erros desse tipo, o processo de seleção foi realizado de forma que quando ocorreram dúvidas na aplicação de algum critério, o estudo não foi eliminado e passou para a próxima fase.

Construção: contempla a relação entre a teoria por trás do experimento e das observações. Mesmo se identificado que existe uma relação casual entre o tratamento do nosso experimento e o resultado observado, o tratamento pode não corresponder à causa que pensamos ter controlado e alterado. Da mesma forma, o resultado observado pode não corresponder ao efeito que pensamos estar medindo. Com o objetivo de minimizar ameaças dessa natureza, foram utilizados sinônimos para as principais palavras-chave, mesmo assim, pode ser que o estudo não tenha encontrado todos os trabalhos sobre o tema.

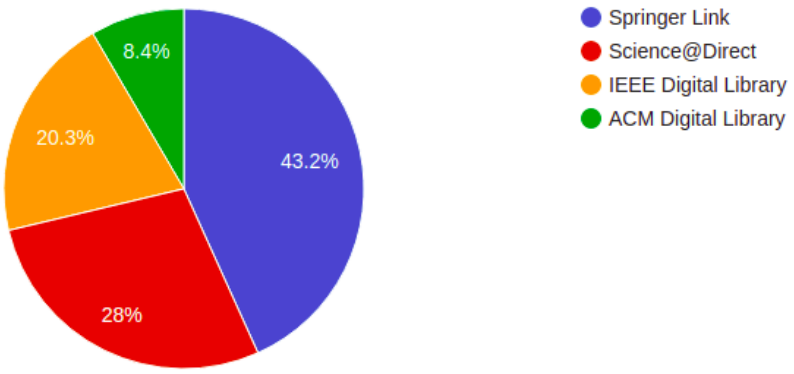
Externas: preocupa-se se podemos generalizar os resultados fora do escopo do nosso estudo. Mesmo se tivermos estabelecido uma relação casual estatisticamente significativa entre um tratamento e um resultado e estes correspondam a causa e efeito que nos propusemos a investigar, os resultados são de pouco uso se a causa e efeito que estabelecemos não se sustentam em outras situações. Esta ameaça foi mitigada com a utilização de critérios de seleção, mesmo assim, mais estudos precisam ser conduzidos para que a generalização dos resultados ocorra.

4. Resultados

Nesta seção serão apresentados os resultados, de acordo com a extração dos dados conduzida durante a RSL.

Utilizando a string de busca definida, conforme apresentado na Seção 3.2, foi realizada, em 06/03/2022, a pesquisa pelos artigos nas fontes de dados selecionadas. Foram retornados 592 trabalhos, sendo esses distribuídos da seguinte forma: 50 na ACM Digital Library, 120 na IEEE Digital Library, 166 na Sience@Direct e 256 na Springer Link, conforme disposto na Figura 4.1.

Figura 4.1 - Distribuição de estudos retornados por fonte de dados.



Fonte: Ferramenta Parsifal.

Após a pesquisa e execução do procedimento de seleção descrito na Seção 3.4, foram selecionados 37 artigos, esses estão listados na Tabela 4.1 e distribuídos da seguinte forma: 7 na ACM Digital Library, 12 na IEEE Digital Library, 10 na Sience@Direct e 8 na Springer Link, conforme disposto na Figura 4.2.

Tabela 4.1 - Artigos selecionados

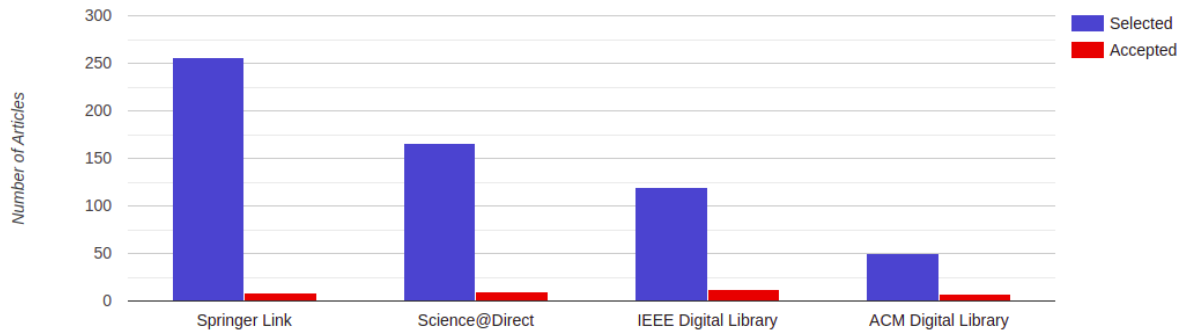
Artigo	**Citação**	**Domínio**
Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges	[1]	*Mobile Banking*
Risk Management for Cloud Compliance with the EU General Data Protection Regulation	[2]	*Cloud*
A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices	[3]	Organizações em geral
GDPR Impact on Computational Intelligence Research	[4]	Pesquisa em Inteligência Computacional
Why you should care about GDPR in IoT Enterprises & Solutions	[5]	*Internet of Things* (IoT)
A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR	[6]	*Blockchain*

GDPR compliance in Video Surveillance and Video Processing Application	[7]	Processamento de vídeo
Development of GDPR-Compliant Software: Document Management System for HR Department	[8]	Departamentos de Recursos Humanos (RH)
Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR	[9]	Pesquisa em *Big Data*
Privacy-awareness of Users in our Cloudy Smart World	[10]	*Cloud*
Privacy in Software Ecosystems - An Initial Analysis of Data Protection Roles and Challenges	[11]	Ecossistemas de *software*
Immutability and Decentralized Storage: An Analysis of Emerging Threats	[12]	*Blockchain*
The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise	[13]	Políticas de privacidade
Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web	[14]	Políticas de privacidade
It's All Fun and Games, and Some Legalese: Data Protection Implications for Increasing Cyber-Skills of Employees through Games	[15]	Organizações em geral
Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control	[16]	Políticas de privacidade
Understanding and Benchmarking the Impact of GDPR on Database Systems	[17]	Sistemas de bancos de dados
An Empirical Study on the Impact of GDPR and Right to Be Forgotten - Organizations and Users Perspective	[18]	Organizações em geral
Digital Retail Challenges within the EU: Fulfillment of Holistic Customer Journey Post GDPR	[19]	Empresas de varejo
How the GDPR can contribute to improving geographical research	[20]	Pesquisa em geografia
Towards privacy compliance: A design science study in a small organization	[21]	Pequenas e médias empresas
A survey on privacy issues and solutions for Voice-controlled Digital Assistants	[22]	Processamento de voz
The impact of the general data protection regulation on innovation and the global political economy	[23]	Política econômica global

Building up the “Accountable Ulysses” model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks	[24]	Pesquisa em saúde
Understanding the notion of risk in the General Data Protection Regulation	[25]	Organizações em geral
Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems	[26]	Assistência médica
Backups and the right to be forgotten in the GDPR: An uneasy relationship	[27]	*Backups*
Accountability of platform providers for unlawful personal data processing in their ecosystems–A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR	[28]	Provedores de plataformas
Information privacy, impact assessment, and the place of ethics	[29]	Organizações em geral
General Data Protection Regulation in Health Clinics	[30]	Assitência médica
The general data protection regulation, the clinical trial regulation and some complex interplay in pediatric clinical trials	[31]	Assitência médica
The influence of GDPR on activities of social enterprises	[32]	Empresas sociais
Two years after: A scoping review of GDPR effects on SeriousGames research ethics reporting	[33]	Pesquisa em geral
What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective	[34]	Pesquisa em saúde
Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR	[35]	Empresas sociais
Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects	[36]	Organizações em geral
International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)	[37]	Pesquisa em assistência médica

Fonte: O autor.

Figura 4.2 - Distribuição de trabalhos selecionados aceitos por fonte de dados.



Fonte: Ferramenta Parsifal.

Os critérios de qualidade descritos na Seção 3.5 auxiliaram na avaliação da importância dos estudos encontrados para este trabalho. A pontuação final de cada artigo está listada na Tabela 4.2.

Tabela 4.2 - Pontuação final referente à avaliação de qualidade dos artigos selecionados.

Artigo	Pontuação Final
[21]	5,0
[14]	4,5
[17]	4,5
[18]	4,5
[6]	4,0
[11]	4,0
[13]	4,0
[16]	4,0
[19]	4,0
[30]	4,0
[2]	3,5
[7]	3,5
[9]	3,5
[10]	3,5
[20]	3,5
[22]	3,5
[26]	3,5
[32]	3,5

[33]	3,5
[1]	3,0
[3]	3,0
[4]	3,0
[5]	3,0
[8]	3,0
[12]	3,0
[15]	3,0
[23]	3,0
[24]	3,0
[25]	3,0
[27]	3,0
[28]	3,0
[29]	3,0
[31]	3,0
[34]	3,0
[35]	3,0
[36]	3,0
[37]	3,0

Fonte: O autor.

Nas próximas seções, serão respondidas as perguntas de pesquisa que foram definidas para esta RSL.

4.1. P1: De acordo com a literatura, qual é o impacto gerado pela GDPR nas Organizações do mundo?

Para identificar o impacto gerado pela GDPR nas Organizações do mundo, foram definidas 3 subperguntas, listadas na Tabela 3.2, relacionadas à pergunta de pesquisa P1. Visto isso, a pergunta P1 será respondida através de uma análise sobre os resultados das subperguntas P1.1, P1.2 e P1.3 nas próximas seções.

4.1.1. P1.1: De acordo com a literatura, quais são as áreas afetadas com a adequação a GDPR?

Dos 37 artigos analisados, foram identificadas 14 áreas afetadas com a necessidade de adequação a GDPR, essas estão listadas na na Tabela 4.3.

Tabela 4.3 - Principais áreas afetadas de acordo com os estudos selecionados.

Identificador	Área	Citações	Quantidade
A1	Pesquisa Acadêmica	[4], [9], [20], [24], [33], [34], [37]	7
A2	Políticas de Privacidade	[13], [14], [16]	3
A3	Assistência Médica	[26], [30], [31]	3
A4	*Cloud*	[2], [10]	2
A5	*IoT*	[5], [10]	2
A6	*Blockchain*	[6], [12]	2
A7	Processamento de Voz e Vídeo	[7], [22]	2
A8	Empresas Sociais	[32], [35]	2
A9	*Mobile Banking*	[1]	1
A10	Recursos Humanos	[8]	1
A11	Bancos de Dados	[17]	1
A12	Empresas de Varejo	[19]	1
A13	Pequenas e Médias Empresas	[21]	1
A14	Sistemas de *Backup*	[27]	1

Fonte: O autor.

Nas próximas seções serão apresentados desafios encontrados e os métodos, tecnologias e práticas utilizadas pelas Organizações na adequação à GDPR.

4.1.2. P1.2: De acordo com a literatura, quais são os desafios que as Organizações encontraram para e com a adequação a GDPR?

Dos 37 artigos analisados, foram identificados 9 desafios enfrentados pelas Organizações no processo de adequação a GDPR, conforme mostrado na Tabela 4.4.

Tabela 4.4 - Desafios enfrentados pelas Organizações mencionados nos estudos selecionados.

Identificador	Desafio	Citações	Quantidade
D1	Disponibilidade de orçamento	[1], [5], [8], [17], [19], [21], [24], [32], [34]	9
D2	Escrever comunicações de consenso de forma clara	[1], [10], [13], [14], [20]	5

D4	Compartilhamento internacional de dados	[1], [18], [19], [20], [24]	5
D3	A legislação não é clara	[1], [17], [18], [26]	4
D5	Dificuldade no processo de anonimização dos dados	[6], [7], [9], [12]	4
D6	Adequação dos *backups*	[18], [27]	2
D7	Não ter uma equipe com expertise sobre a lei	[5], [21]	2
D8	Utilização de serviços de terceiros	[14], [18]	2
D9	Sistemas passam a perder performance	[17]	1

Fonte: O autor.

Nas próximas seções, serão apresentadas as referências relacionadas a cada um dos desafios encontrados.

a) Disponibilidade de orçamento (D1)

Dos desafios mapeados, D1 foi o mais citado com 9 menções. As afirmações que permitiram a conclusão da existência deste desafio foram:

- [1], [5], [8], [24] e [34] citam como um dos desafios organizacionais o planejamento para investimentos adicionais decorrentes da adequação;
- [21] menciona o investimento necessário para a adequação como um grande desafio para Pequenas e Médias Empresas (PME);
- [17] argumenta que o conceito de privacidade por design e por padrão estabelecido pela GDPR está em desacordo com o tradicional objetivo das Organizações de otimizar gastos;
- [19] afirma que a adequação pode custar para as empresas de varejo muitos recursos e oportunidades de aumento de receita;
- [32] cita os custos de execução para a adequação como uma dificuldade encontrada por Empresas Sociais.

b) Escrever comunicações de consenso de forma clara (D2)

A dificuldade de Escrever comunicações de consenso de forma clara (D2) é mencionada em 5 estudos::

- [1], [10]. [13], [14] e [20] citaram como dificuldade escrever comunicações de consentimento claras, inequívocas, em linguagem simples e em formato simples, pois, caso contrário, o consentimento se tornará inválido.

c) A legislação não é clara (D3)

O desafio D3 é mencionado em 4 estudos:

- [1] cita que um desafio organizacional é o fato da GDPR não fornecer orientação clara sobre como ou qual é o método mais eficiente de desidentificação de dados;
- [17] argumenta que vários regulamentos da GDPR são intencionalmente vagos em suas especificações técnicas para acomodar futuros avanços em tecnologias e que muitos requisitos estão fundamentalmente em desacordo com os princípios de design e práticas operacionais de sistemas de computação modernos;
- [18] alega que a legislação carece de instruções precisas sobre como um operador de dados pode garantir que todas as informações pessoais do titular dos dados sejam excluídas, considerando a quantidade de dados, e-mail e backups comuns nos sistemas de informação atuais;
- [26] menciona como um problema crítico a definição de processamento no contexto de assistência média, pois na área da saúde, esse pode se referir a um percurso de cuidados específico, a todo um ambulatório ou a um exame de diagnóstico de um único paciente.

d) Compartilhamento internacional de dados (D4)

A dificuldade no compartilhamento internacional de dados (D4) está presente em 5 trabalhos:

- [1] e [18] citam como um dos desafios organizacionais, o fato de Organizações sediadas fora da União Européia, envolvidas na coleta de dados, terem de seguir a lei e assegurar seus requisitos. Complementando, [19] argumenta que muitas empresas globais terceirizam suas atividades de processamento de dados em países de baixo custo. O escopo territorial da GDPR abrange até mesmo países não pertencentes à União Europeia, desde que os titulares dos dados sejam residentes. Isso significa que os controladores de dados terão que garantir que esses operadores de dados terceirizados estejam em conformidade com o GDPR, o que é um desafio para essas empresas;
- [20] e [24] alegam que a GDPR padronizou a legislação no nível europeu, mas ao mesmo tempo permitiu que os Estados-Membros especificassem nacionalmente as condições e requisitos no contexto do processamento de dados para fins de pesquisa científica e estatística. Fato que cria um obstáculo por tais atividades serem frequentemente conduzidas por parcerias pertencentes a diferentes nacionalidades, dificultando o trabalho de campo internacional e a colaboração acadêmica.

e) Dificuldade no processo de anonimização dos dados (D5)

A anonimização dos dados (D5) é discutida em 4 trabalhos:

- [6] e [12] citam que em sistemas *blockchain*, uma tentativa de alterar os dados existentes fará com que a *hash* do bloco de dados correspondente não corresponda mais ao valor da *hash* incluída no próximo bloco, quebrando assim a cadeia. Essa característica de imutabilidade tem sido discutida como uma das principais preocupações sobre a conformidade com a GDPR por parte dos sistemas *blockchain*;

- [9] elenca como dificuldade relacionada ao conjunto de dados, o fato de que, mesmo que os parâmetros diretamente identificáveis sejam removidos no processo de anonimização, ainda pode ser possível reidentificar indivíduos únicos, combinando o conjunto de dados com outras informações.
- [7] argumenta que alcançar uma anonimização real dos dados oriundos de vigilância em vídeo é difícil de ser executada;

f) Adequação dos backups (D6)

A Adequação dos backups (D6) é mencionada em 2 trabalhos:

- [18] e [27] argumentam que um dos maiores desafios do conceito de *right to be forgotten* definido na GDPR é a adequação dos *backups*. Excluir dados de *backups* é uma tarefa muito difícil para Organizações. A remoção de informações pessoais do usuário de arquivos ou *backups* só pode ser feita durante o processo de restauração dos dados. A legislação não diz especificamente que precisa remover dados pessoais dos *backups*, mas uma vez que um *backup* é restaurado, todos os dados que qualquer indivíduo pediu para excluir não podem ser recuperados. Como as Organizações podem acompanhar isso? Será uma tarefa tediosa.

g) Não ter uma equipe com expertise sobre a lei (D7)

A dificuldade de ter uma equipe que conheça a lei é reportada em 2 estudos:

- [5] cita como um dos desafios primários relacionados a conformidade, a falta de pessoal especializado;
- [21] elenca como um dos desafios identificados por PME para a adequação, ter uma equipe com conhecimentos limitados sobre os requisitos da lei.

h) Utilização de serviços de terceiros (D8)

A Utilização de serviços de terceiros (D8) é descrita em 2 estudos:

- [14] alega que muitas das coletas de dados que acontecem em websites são realizadas automaticamente por terceiros. O problema com terceiros nesse contexto, vem do fato de que, mesmo que os rastreadores de terceiros sejam definidos apenas após o consentimento do usuário, a GDPR exige que o consentimento possa ser retirado e, portanto, os dados obtidos devem ser excluídos. Como os dados não são armazenados pela parte que administra o site, eles não têm acesso direto a eles e o que podem fazer é solicitar uma exclusão. Fato que evidencia uma falta de controle direto sobre dados pessoais dos usuários;
- [18] menciona que com o desenvolvimento e o aumento do uso de serviços em *cloud*, empresas estão cada vez mais migrando a implementação de seus sistemas para essa tecnologia, mas que a confiança sobre a utilização dos dados do usuário é construída entre esse e a organização e não entre o usuário e o provedor *cloud*. Com isso, muitas vezes, os usuários nem são informados de que a organização está hospedando seus

dados na nuvem. Ter que informar os usuários sobre todos os eventuais serviços de terceiros sendo utilizados é um desafio para Organizações.

i) Sistemas passam a perder performance (D9)

A performance dos sistemas é mencionada em 1 trabalho:

- [17] observa que os objetivos de privacidade por design e por padrão estabelecidos pela GDPR se opõem ao tradicional design orientado a performance dos sistemas. Por exemplo, para notificar usuários afetados por um eventual vazamento de dados, uma empresa deve manter registros de todos os acessos a tais dados pessoais, na perspectiva de bancos de dados, isso ocasiona que toda operação de leitura seja seguida de uma operação de escrita, fato que impacta diretamente na performance desses bancos.

4.1.3. P1.3: De acordo com a literatura, quais são os métodos/tecnologias/práticas que as Organizações utilizam para a adequação a GDPR?

Dos 37 artigos analisados, foram identificados 9 métodos, tecnologias e práticas utilizadas para a adequação a GDPR, conforme mostrado na Tabela 4.5.

Tabela 4.5 - Métodos/tecnologias/práticas mencionadas nos estudos selecionados

Identificador	Métodos/tecnologias/práticas	Citações	Quantidade
MTP1	Criptografia	[2], [6], [9], [12], [18], [19], [36]	7
MTP2	Pseudonimização e anonimização	[2], [7], [9], [19], [22]	5
MTP3	Desenvolvimento de um *software* próprio	[8], [17], [20], [21], [24]	5
MTP4	Registros de acesso	[2], [8], [30]	3
MTP5	Adoção de *frameworks*	[5], [8], [26]	3
MTP6	Treinamento da equipe	[4], [30]	2
MTP7	Utilização de *smart contracts*	[6], [12]	2
MTP8	Opção por provedores cloud adequados à GDPR	[18]	1
MTP9	Não coletar dados desnecessários	[19]	1

Fonte: O autor.

Nas próximas seções, serão apresentadas as referências relacionadas a cada um dos métodos, tecnologias e práticas encontradas.

a) Criptografia (MTP1)

Dos métodos, tecnologias e práticas mapeadas, MTP1 foi a mais mencionada, com 7 citações. Tais estão listadas abaixo:

- [2] e [9] citam que serviços *cloud* podem evitar falhas de proteção de informações pessoais, garantindo a utilização de uma criptografia adequada para todos os dados que estão sendo transitados ou em repouso;
- [6] e [12] mencionam que uma solução para o problema relacionado a imutabilidade dos sistemas *blockchain,* seria armazenar os dados de forma criptografada ou armazenar dados fora da cadeia, mantendo seus *hashes* na *blockchain*;
- [18] sugere a utilização de um apagamento criptografado, em que cada registro é criptografado com uma chave única, portanto, quando as solicitações de apagamento de dados são recebidas, a chave é destruída, resultando na inutilização desses dados;
- [19] afirma que ao processar dados entre canais, os varejistas digitais devem garantir que seus sistemas e aplicativos estejam em conformidade com a privacidade por design e por padrão. Isso pode ser alcançado por meio de algumas práticas simples, como criptografia de dados confidenciais, como o PIN de cartões de crédito e débito;
- [36] sugere a utilização de criptografia de dados, o que permite que as operações de análise sejam executadas sem exposição dos dados por parte das Organizações.

b) Pseudonimização e anonimização (MTP2)

Dos métodos, tecnologias e práticas mapeadas, MTP2 recebeu 5 menções. Tais estão listadas abaixo:

- [2], [9] e [19] citam a utilização de pseudominimização e anonimização como formas válidas de conformidade;
- [7] sugere a utilização de camadas extras de filtragem e efeitos que impedem a identificação de indivíduos em sistemas de vídeo, tanto gravados quanto transmissões ao vivo;
- [22] alega que, para proteger a privacidade dos usuários em sistemas de processamento de voz, ofuscam e removem características sensíveis da voz do usuário.

c) Desenvolvimento de um *software* próprio (MTP3)

Dos métodos, tecnologias e práticas mapeadas, MTP3 recebeu 5 menções. Tais estão listadas abaixo:

- [8] cita que para adequar o processo de aplicação de empregos feito pelo departamento de Recursos Humanos de empresas aos princípios da GDPR, foi desenvolvido um *software* próprio para apoiar os processos mais comuns dessa atividade;
- [17] sugere que, para alcançar conformidade em bancos de dados, seja utilizado um *software* desenvolvido pelos autores que modela consultas e cargas de trabalho que os

bancos de dados encontram no mundo real e desenvolve métricas para representar sucintamente seu comportamento;

- [20] menciona que o departamento de TI de sua instituição desenvolveu um *software* que permite armazenar e analisar dados pessoais de maneira segura e em conformidade com a GDPR;
- [21] desenvolveu um *software* para os colaboradores conduzirem testes automatizados dos requerimentos de privacidade determinados pela GDPR;
- [24] criou um *software* que adota medidas técnicas e organizacionais adequadas e eficazes para garantir o cumprimento ético-legal das diretrizes estabelecidas pela GDPR.

d) Registros de acesso (MTP4)

Dos métodos, tecnologias e práticas mapeadas, MTP4 recebeu 3 menções. Tais estão listadas abaixo:

- [2], [8] e [30] utilizam *logs*, onde serão registradas todas as atividades possíveis do sistema, tais como: login, inserção, visualização, edição, remoção e impressão de dados ou arquivos.

e) Adoção de *frameworks* (MTP5)

Dos métodos, tecnologias e práticas mapeadas, MTP5 recebeu 3 menções. Tais estão listadas abaixo:

- [5] e [8] sugerem a utilização da ISO 27001 para adequação à GDPR, que fornece evidências significativas de que uma entidade está em conformidade com a lei.
- [26] desenvolveu um protocolo específico para sistemas de informação sobre assistência médica serem capazes de se adequar à legislação. Tal metodologia foi aplicada com sucesso em um ambiente real, apoiando assim sua validade e capacidade de destacar riscos em *softwares* e sistemas;

f) Treinamento da equipe (MTP6)

Dos métodos, tecnologias e práticas mapeadas, MTP6 recebeu 2 menções. Tais estão listadas abaixo:

- [4] alega que, no campo de Pesquisa em Inteligência Computacional, uma medida para adequação é garantir que o time de pesquisadores tenha um treinamento apropriado sobre o que determina a GDPR;
- [30] sugere que treinamentos e sessões de conscientização devem ser realizados a fim de evitar violações.

g) Utilização de *smart contracts* (MTP7)

Dos métodos, tecnologias e práticas mapeadas, MTP7 recebeu 2 menções. Tais estão listadas abaixo:

- [6] e [12] explicam que em uma *blockchain* pública, uma vez que uma transação tenha sido feita, o mesmo conjunto de dados será processado por todos os nós da cadeia. Consequentemente, obter o consentimento explícito é essencial no início antes do download ou execução da *blockchain*. Na literatura, existem estudos enfatizando que cada transação executada precisa incluir uma declaração de consentimento para ser aceita pelos titulares dos dados, o que pode ser difícil de gerenciar para a maioria dos sistemas públicos de *blockchain*. Uma solução proposta para esse problema é usar *smart contracts* para lidar automaticamente com o gerenciamento de consentimento.

h) Opção por provedores *cloud* adequados à GDPR (MTP8)

A opção por provedores cloud adequados à GDPR (MTP8) é mencionada no trabalho [18] que sugere que as Organizações devem migrar para provedores de serviços *cloud* que já estejam em conformidade com o GDPR;

i) Não coletar dados desnecessários (MTP9)

Dos métodos, tecnologias e práticas mapeadas, MTP9 recebeu 1 menção. Tal está listada abaixo:

- [19] argumentam que os varejistas digitais devem minimizar a quantidade de dados coletados, não coletando dados de identificação pessoal desnecessariamente para minimizar vulnerabilidades. Além disso, os varejistas digitais podem permitir que os titulares dos dados façam alguns compartilhamentos por conta própria, como postar seus dados pessoais, fotos, exclusão de informações, etc. Isso pode ser feito nas instalações de mídia social da empresa, como página corporativa do Facebook, identificador do Twitter, LinkedIn e assim por diante. Ao fazer isso, os clientes desfrutarão de jornadas interativas, mas serão responsáveis por sua própria privacidade de dados.

4.2. Análise dos Resultados

Realizando uma análise sobre os resultados apresentados na Seção 4.1, é possível mapear desafios encontrados e métodos, tecnologias e práticas utilizadas por cada uma das áreas levantadas. Essas informações são apresentadas na Tabela 4.6.

Tabela 4.6 - Análise dos resultados

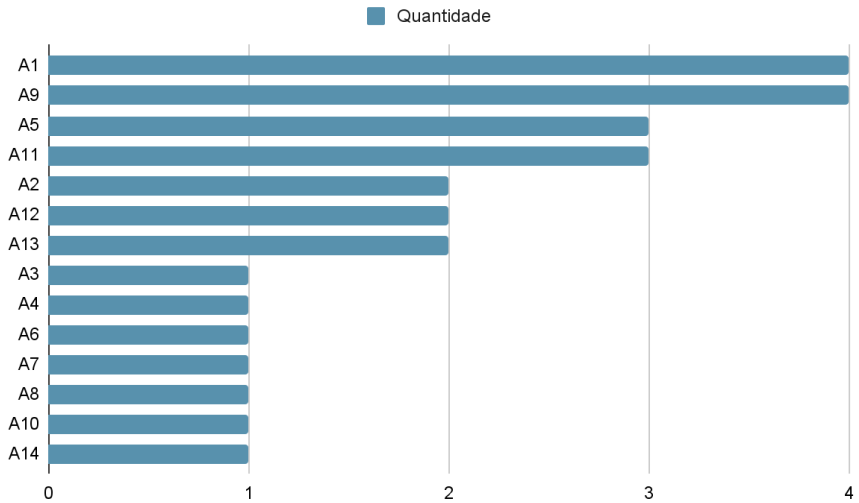
Área	**Desafios**	**Citações dos Desafios**	**Métodos/tecnologias/ práticas**	**Citações dos métodos/tecnologias/práticas**
A1	D1, D2, D4, D5	[9], [20], [24], [34]	MTP1, MTP2, MTP3, MTP6	[4], [9], [20], [24]
A2	D2, D8	[13], [14]	-	-
A3	D3	[26]	MTP4, MTP5, MTP6	[26], [30]

A4	D2	[10]	MTP1, MTP2, MTP4	[2]
A5	D1, D2, D7	[5], [10]	MTP5	[5]
A6	D5	[6], [17]	MTP1, MTP7	[6], [12]
A7	D5	[7]	MTP2	[7], [22]
A8	D1	[32]	-	-
A9	D1, D2, D3, D4	[1]	-	-
A10	D1	[8]	MTP3, MTP4, MTP5	[8]
A11	D1, D3, D9	[17]	MTP3	[17]
A12	D1, D4	[19]	MTP1, MTP2, MTP9	[19]
A13	D1, D7	[21]	MTP3	[21]
A14	D6	[27]	-	-

Fonte: O autor.

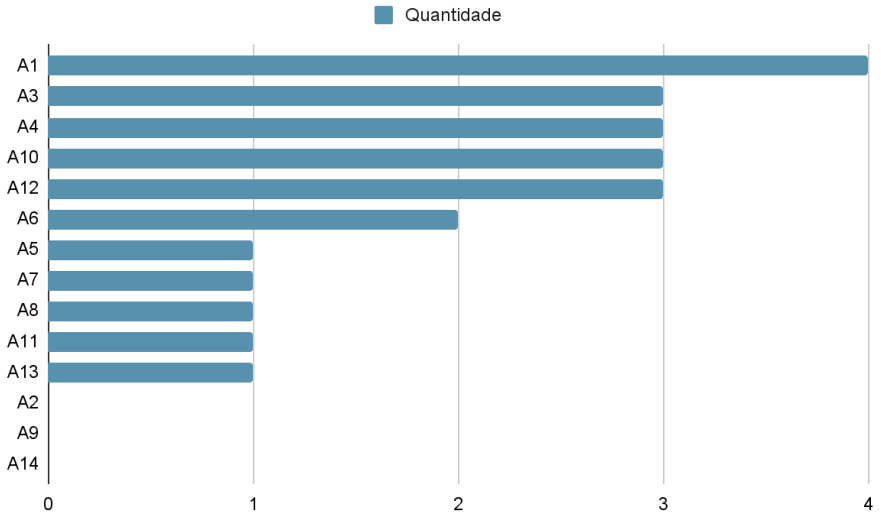
Na Figura 4.3 e Figura 4.4 são detalhadas as quantidades de desafios encontrados e métodos, tecnologias e práticas utilizadas por cada área, respectivamente. Através da Figura 4.6, nota-se que as áreas de Pesquisa Acadêmica (A1) e *Mobile Banking* (A9) foram as que encontraram mais desafios, com 5 citações. Com a Figura 4.7, percebe-se que a área de Pesquisa Acadêmica (A1) foi a que mais utilizou métodos, tecnologias e práticas diferentes, com 4 citações.

Figura 4.3 - Quantidade de desafios encontrados por área



Fonte: O autor.

Figura 4.4 - Quantidade de métodos/tecnologias/práticas utilizados por área



Fonte: O autor.

Pela Tabela 4.6, também é interessante destacar que as áreas de Políticas de Privacidade (A2), Empresas Sociais (A8), *Mobile Banking* (A9) e Sistemas de *Backup* (A14), embora mencionaram desafios encontrados, não citaram métodos, tecnologias e práticas sendo utilizadas atualmente. Fato que pode estar indicando uma necessidade de soluções para esses segmentos.

Nas próximas seções, serão detalhados os desafios e métodos, tecnologias e práticas utilizadas por cada uma das áreas mapeadas.

a) Pesquisa Acadêmica (A1)

Os trabalhos analisados na área de Pesquisa Acadêmica citaram como desafios organizacionais: o planejamento para investimentos adicionais decorrentes da adequação à GDPR (D1) [24][34], a dificuldade na escrita de comunicações de consenso de forma clara, inequívoca e em linguagem simples (D2) [20], desafios no contexto de compartilhamento de dados internacional, pelo fato de que Estados-Membros podem especificar nacionalmente as condições e requisitos no contexto do processamento de dados para fins de pesquisa científica e estatística, o que cria um obstáculo por tais atividades serem frequentemente conduzidas por parcerias pertencentes a diferentes nacionalidades, dificultando o trabalho de campo internacional e a colaboração acadêmica (D4) [20][24]. O campo de Pesquisa em *Big Data* elenca como dificuldade relacionada a conjunto de dados, o fato de que, mesmo que os parâmetros diretamente identificáveis sejam removidos no processo de anonimização, ainda pode ser possível reidentificar indivíduos únicos, combinando o conjunto de dados com outras informações (D5) [9]. Formas de mitigação identificadas foram o fato de que serviços *cloud* podem evitar falhas de proteção de informações pessoais, garantindo a utilização de criptografia adequada para todos os dados que estão sendo transitados ou em repouso (MTP1), utilização de pseudonimização e anonimização (MTP2), desenvolvimento de softwares próprios (MTP3) e garantir que o time de pesquisadores tenha um treinamento apropriado sobre o que determina a GDPR (MTP6).

b) Políticas de Privacidade (A2)

Os artigos analisados na área de Políticas de Privacidade citam como dificuldade: escrever comunicações de consentimento claras, inequívocas e em linguagem simples, pois, caso contrário, o consentimento se tornará inválido (D2) [13][14]. Além disso, é mencionado que muitas das coletas de dados que acontecem em websites são realizadas automaticamente por terceiros. O problema com terceiros nesse contexto, vem do fato de que, mesmo que os rastreadores de terceiros sejam definidos apenas após o consentimento do usuário, a GDPR exige que o consentimento possa ser retirado e, portanto, os dados obtidos devem ser excluídos. Como os dados não são armazenados pela parte que administra o site, eles não têm acesso direto a eles e a única ação que podem realizar é a solicitação de exclusão. Fato que evidencia uma falta de controle direto sobre dados pessoais dos usuários (D8). Não foram identificadas formas de mitigação para os desafios encontrados.

c) Assistência Médica (A3)

O desafio identificado na área de Assistência Médica é a definição de processamento no contexto de assistência médica, pois na área da saúde, esse pode se referir a um percurso de cuidados específico, a todo um ambulatório ou a um exame de diagnóstico de um único paciente (D3) [26]. Como mitigações, foram identificados a utilização de *logs*, onde serão registradas todas as atividades possíveis do sistema, tais como: login, inserção, visualização, edição, remoção e impressão de dados ou arquivos (MTP4) [30], o desenvolvimento de um protocolo específico para sistemas de informação sobre assistência médica serem capazes de se adequar à legislação (MTP5) e a realização de treinamentos e sessões de conscientização a fim de evitar violações (MTP6) [30].

d) *Cloud* (A4)

O desafio identificado na área de *Cloud* foi a dificuldade em escrever comunicações de consentimento claras, inequívocas e em linguagem simples (D2) [10]. Como formas de adequação identificadas, estão o fato de serviços *cloud* poderem evitar falhas de proteção de informações pessoais, garantindo a utilização de uma criptografia adequada para todos os dados que estão sendo transitados ou em repouso (MTP1), utilização de pseudominimização e anonimização (MTP2) e utilização de *logs*, onde serão registradas todas as possíveis atividades de um sistema (MTP4) [2].

e) *IoT* (A5)

Desafios identificados em *IoT* foram o planejamento para investimentos adicionais decorrentes da adequação (D1) [5], escrever comunicações de consentimento claras, inequívocas, em linguagem simples e em formato simples (D2) [10] e a falta de pessoal especializado (D7). Como forma de mitigação, foi identificado o uso da ISO 27001 para

adequação à GDPR, que fornece evidências significativas de que uma entidade está em conformidade com a lei (MTP5).

f) *Blockchain* (A6)

Para a área de *Blockchain* o desafio encontrado foi o fato de que em sistemas *blockchain*, uma tentativa de alterar os dados existentes fará com que a *hash* do bloco de dados correspondente não corresponda mais ao valor da *hash* incluída no próximo bloco, quebrando assim a cadeia. Essa característica de imutabilidade tem sido discutida como uma das principais preocupações sobre a conformidade com a GDPR por parte dos sistemas *blockchain* (D5) [6][12]. Uma solução para o problema relacionado à imutabilidade dos sistemas *blockchain*, seria armazenar os dados de forma criptografada ou armazenar dados fora da cadeia, mantendo seus hashes na *blockchain* (MTP1). Além disso, em uma *blockchain* pública, uma vez que uma transação tenha sido feita, o mesmo conjunto de dados será processado por todos os nós da cadeia. Consequentemente, obter o consentimento explícito é essencial no início antes do *download* ou execução da *blockchain*. Na literatura, existem estudos enfatizando que cada transação executada precisa incluir uma declaração de consentimento para ser aceita pelos titulares dos dados, o que pode ser difícil de gerenciar para a maioria dos sistemas públicos de *blockchain*. Uma solução proposta para esse problema é usar *smart contracts* para lidar automaticamente com o gerenciamento de consentimento (MTP7).

g) Processamento de Voz e Vídeo (A7)

Para o Processamento de Voz e Vídeo, a literatura cita que uma anonimização real dos dados dados oriundos de vigilância em vídeo é difícil de ser executada (D5) [7]. Formas de mitigação para os desafios encontrados na área, são a utilização de camadas extras de filtragem e efeitos que impedem a identificação de indivíduos em sistemas de vídeo, tanto gravados quanto transmissões ao vivo, e ofuscar e remover características sensíveis da voz de usuários (MTP2) [22].

h) Empresas Sociais (A8)

O desafio identificado para as Empresas Sociais foram os custos de execução para a adequação (D1) [32]. Para esse desafio, não foram identificadas formas de mitigação.

i) Mobile Banking (A9)

A área de *Mobile Banking* identificou como desafios: o planejamento para investimentos adicionais decorrentes da adequação (D1) [1], escrever comunicações de consentimento claras, inequívocas, em linguagem simples e em formato simples (D2), o fato da GDPR não fornecer orientação clara sobre como ou qual é o método mais eficiente de desidentificação de dados (D3) e o fato de Organizações sediadas fora da União Européia,

envolvidas na coleta de dados, terem de seguir a lei e assegurar seus requisitos (D4). Para esses desafios, não foram identificadas formas de mitigação.

j) Recursos Humanos (A10)

O desafio identificado para a área de Recursos Humanos é o investimento necessário para a adequação (D1) [8]. Como mitigação, para adequar o processo de aplicação de empregos feito pelo departamento de Recursos Humanos de empresas aos princípios da GDPR, foi desenvolvido um *software* próprio para apoiar os processos mais comuns dessa atividade (MTP3). Além disso, *logs* são utilizados, onde serão registradas todas as atividades possíveis em um sistema (MTP4). Por fim, também foi identificada a utilização da ISO 27001 no processo de adequação à GDPR, que fornece evidências significativas de que uma entidade está em conformidade com a lei (MTP5).

h) Bancos de Dados (A11)

Dentre os desafios encontrados na adequação de Bancos de Dados estão: o fato do conceito de privacidade por design e por padrão estabelecido pela GDPR estar em desacordo com o tradicional objetivo das Organizações de otimizar gastos (D1) [17] e vários regulamentos da GDPR serem intencionalmente vagos em suas especificações técnicas para acomodar futuros avanços em tecnologias, além de muitos requisitos estarem fundamentalmente em conflito com os princípios de design e práticas operacionais de sistemas de computação modernos (D3). Observa-se também que os objetivos de privacidade por design e por padrão estabelecidos pela GDPR se opõem à performance dos sistemas. Por exemplo, para notificar usuários afetados por um eventual vazamento de dados, uma empresa deve manter registros de todos os acessos a tais dados pessoais, na perspectiva de bancos de dados, isso torna toda operação de leitura, numa operação de leitura seguida de uma operação de escrita, fato que impacta diretamente na performance desses bancos (D9). Uma prática utilizada para alcançar conformidade em bancos de dados, é utilizar um *software* que modela consultas e cargas de trabalho que os bancos de dados encontram no mundo real e desenvolve métricas para representar sucintamente seu comportamento (MTP3).

l) Empresas de Varejo (A12)

Dentre os desafios encontrados por Empresas de Varejo estão os custos com a adequação (D1) e o fato de que muitas empresas globais terceirizam suas atividades de processamento de dados em países de baixo custo [19]. O escopo territorial da GDPR abrange até mesmo países não pertencentes à União Europeia, desde que os titulares dos dados sejam residentes. Isso significa que os controladores de dados terão que garantir que esses processadores de dados terceirizados estejam em conformidade com a GDPR, o que é um desafio para essas empresas (D4). Como forma de mitigação para esses desafios, ao processar dados entre canais, os varejistas digitais devem garantir que seus sistemas e aplicativos estejam em conformidade com a privacidade por design e por padrão. Isso pode ser alcançado por meio de algumas práticas simples, como criptografia de dados

confidenciais, como o PIN de cartões de crédito e débito, (MTP1) pseudominimização e anonimização (MTP2). Além disso, os varejistas digitais devem minimizar a quantidade de dados coletados, não coletando dados de identificação pessoal desnecessariamente para minimizar vulnerabilidades. Além disso, os varejistas digitais podem permitir que os titulares dos dados façam alguns compartilhamentos por conta própria, como postar seus dados pessoais, fotos, exclusão de informações, etc. Isso pode ser feito nas instalações de mídia social da empresa, como página corporativa do Facebook, identificador do Twitter, LinkedIn e assim por diante. Ao fazer isso, os clientes desfrutarão de jornadas interativas, mas serão responsáveis por sua própria privacidade de dados (MTP9).

m) Pequenas e Médias Empresas (A13)

Dentre os desafios encontrados por PME estão o investimento necessário para a adequação (D1) e ter uma equipe com conhecimentos limitados sobre os requisitos da lei (D7) [21]. Uma forma de mitigação identifica na área foi o desenvolvimento um *software* para os colaboradores conduzirem testes automatizados dos requerimentos de privacidade determinados pela GDPR (MTP3).

n) Sistemas de *Backup* (A14)

Para a área de Sistemas de *Backup*, o maior desafio identificado foi a exclusão de dados [27]. A remoção de informações pessoais do usuário de arquivos ou *backups* só pode ser feita durante o processo de restauração dos dados. A legislação não diz especificamente que é preciso remover dados pessoais dos backups, mas uma vez que um *backup* é restaurado, todos os dados que qualquer indivíduo pediu para excluir não podem ser recuperados. Acompanhar tal tarefa é um problema para as Organizações (D6). Não foram identificadas formas de mitigação para o desafio encontrado.

5. Conclusões

Neste trabalho, foi conduzida uma Revisão Sistemática da Literatura com o objetivo de compreender o impacto da adequação à GDPR pelas Organizações. As principais conclusões obtidas foram:

- A área mais mencionada de acordo com os estudos selecionados foi a de Pesquisa Acadêmica (A1), sendo citada 7 vezes. Essa também foi a que enfrentou mais desafios diferentes, com 4, sendo esses: disponibilidade de orçamento (D1), dificuldade na escrita de comunicações de consenso de forma clara (D2), dificuldades relacionadas ao compartilhamento internacional de dados (D4) e o processo de anonimização dos dados (D5). Além disso, essa foi a área que aplicou mais métodos, tecnologias e práticas diferentes, sendo essas: criptografia (MTP1), pseudonimização e anonimização (MTP2), desenvolvimento de um *software* próprio (MTP3) e treinamento da equipe (MTP6);

- Os desafio mais enfrentado pelas Organizações é o de disponibilidade de orçamento (D1), sendo citada 9 vezes;
- O método/tecnologia/prática utilizada pelas Organizações mais citada foi a de criptografia (MTP1), sendo mencionada 7 vezes;
- Foi possível identificar que as áreas de Políticas de Privacidade (A2), Empresas Sociais (A8), *Mobile Banking* (A9) e Sistemas de *Backup* (A14), embora mencionaram desafios encontrados, não citaram métodos, tecnologias e práticas sendo utilizadas atualmente. Fato que pode estar indicando uma necessidade mais urgente de soluções para esses segmentos;

5.1. Contribuições da Pesquisa

Visto isso, pode-se concluir que esta RSL contribuiu para o estado da arte e da prática com a obtenção de um panorama do processo de adequação e respectivo impacto gerado pela GDPR nas Organizações. Com este trabalho, foram mapeadas áreas afetadas, desafios encontrados e métodos, tecnologias e práticas utilizadas pelas Organizações na adequação à GDPR.

A partir dessas informações, torna-se possível a identificação das áreas que sofreram um maior impacto com a legislação, dos desafios principais encontrados e o que foi mais utilizado como forma de mitigação para esses problemas identificados.

Nesse contexto, Organizações que estão procurando se adequar à GDPR podem utilizar este trabalho, a fim de identificar problemas comuns que possam vir a enfrentar e possíveis soluções para serem aplicadas.

Além disso, conseguiu-se identificar áreas que apresentaram problemas, mas ainda não encontraram nenhum tipo de solução para esses, o que pode estar evidenciando segmentos que precisam de uma maior atenção neste momento.

5.2. Trabalhos Futuros

A partir da condução deste trabalho e dos resultados obtidos, os seguintes direcionamentos para novos trabalhos são propostos:

- Ampliar a pesquisa por artigos utilizando outras bases de dados além das utilizadas nesta RSL e, além disso, buscar por publicações em idiomas diferentes do português e inglês;
- Validar os dados mapeados neste trabalho conduzindo entrevistas e questionários;
- Desenvolver métodos/tecnologias/práticas, diferentes das identificadas, que mitiguem os desafios encontrados pelas Organizações na adequação à GDPR;
- Desenvolver soluções que mitiguem os desafios encontrados para as áreas que não citaram nenhum tipo de métodos/tecnologias/práticas.

REFERÊNCIAS

[1] Lakshmi, K. Krithiga and Gupta, Himanshu and Ranjan, Jayanthi et al. Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges. In: 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE Xplore, 2020.

[2] Duncan, Bob and Zhao, Yuan et al. Risk Management for Cloud Compliance with the EU General Data Protection Regulation. In: International Conference on High Performance Computing & Simulation. IEEE Xplore, 2018.

[3] Layton, Roslyn and Elaluf-Calderwood, Silvia et al. A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices. 2019.

[4] Crockett, Keeley and Goltz, Sean and Garratt, Matt et al. GDPR Impact on Computational Intelligence Research. 2018.

[5] Pires, Filipe and Pacheco, Osvaldo R. and Martins, Ricardo T. et al. Why you should care about GDPR in IoT Enterprises & Solutions. 2021.

[6] Belen Sağlam, Rahime and Aslan, Çağri Burak and Li, Shujun and Dickson, Lisa and Pogrebna, Ganna et al. A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR. 2020.

[7] Barnoviciu, Eduard and Ghenescu, Veta and Carata, Serban-Vasile and Ghenescu, Marian and Mihaescu, Roxana and Chindea, Mihai et al. GDPR compliance in Video Surveillance and Video Processing Application. 2019.

[8] Gonçalves, Emanuel and Teixeira, Paulo and Silva, Joaquim P. et al. Development of GDPR-Compliant Software: Document Management System for HR Department. 2020.

[9] Gruschka, Nils and Mavroeidis, Vasileios and Vishi, Kamer and Jensen, Meiko et al. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. 2018.

[10] Varkonyi, G. Gultekin and Kertesz, A. and Varadi, Sz. et al. Privacy-awareness of Users in our Cloudy Smart World. 2019.

[11] Valença, George and Kneuper, Ralf and Rebelo, Maria Eduarda et al. Privacy in Software Ecosystems - An Initial Analysis of Data Protection Roles and Challenges. 2020.

[12] Casino, Fran and Politou, Eugenia and Alepis, Efthimios and Patsakis, Constantinos et al. Immutability and Decentralized Storage: An Analysis of Emerging Threats. 2020.

[13] Zaeem, Razieh Nokhbeh and Barber, K. Suzanne et al.The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. 2020.

[14] Kretschmer, Michael and Pennekamp, Jan and Wehrle, Klaus et al. Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. In: ACM Trans. Web. 2021.

[15] Povse, Danaja Fabcic et al. It's All Fun and Games, and Some Legalese: Data Protection Implications for Increasing Cyber-Skills of Employees through Games. In: Association for Computing Machinery. 2018.

[16] Sanchez-Rola, Iskander and Dell'Amico, Matteo and Kotzias, Platon and Balzarotti, Davide and Bilge, Leyla and Vervier, Pierre-Antoine and Santos, Igor et al. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In: Association for Computing Machinery. 2019.

[17] Shastri, Supreeth and Banakar, Vinay and Wasserman, Melissa and Kumar, Arun and Chidambaram, Vijay et al. Understanding and Benchmarking the Impact of GDPR on Database Systems. In: Proc. VLDB Endow. 2020.

[18] Mangini, Vincenzo and Tal, Irina and Moldovan, Arghir-Nicolae et al. An Empirical Study on the Impact of GDPR and Right to Be Forgotten - Organizations and Users Perspective. In: Association for Computing Machinery. 2020.

[19] Nabbosa, Veronica L. and Iftikhar, Rehan et al. Digital Retail Challenges within the EU: Fulfillment of Holistic Customer Journey Post GDPR. In: Association for Computing Machinery. 2019.

[20] Louise Meijering and Tess Osborne and Esther Hoorn and Cristina Montagner et al. How the GDPR can contribute to improving geographical research. In: Geoforum. 2020.

[21] Ze Shi Li and Colin Werner and Neil Ernst and Daniela Damian et al. Towards privacy compliance: A design science study in a small organization. In: Information and Software Technology. 2022.

[22] Luca Hernández Acosta and Delphine Reinhardt et al. A survey on privacy issues and solutions for Voice-controlled Digital Assistants. In: Pervasive and Mobile Computing. 2022.

[23] Crispin Niebel et al. The impact of the general data protection regulation on innovation and the global political economy. In: Computer Law & Security Review. 2021.

[24] Denise Amram et al. Building up the “Accountable Ulysses” model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks. In: Computer Law & Security Review. 2020.

[25] Raphaël Gellert et al. Understanding the notion of risk in the General Data Protection Regulation. In: Computer Law & Security Review. 2018.

[26] Marco Todde and Marco Beltrame and Sara Marceglia and Cinzia Spagno et al. Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. In: Informatics in Medicine Unlocked. 2020.

[27] Eugenia Politou and Alexandra Michota and Efthimios Alepis and Matthias Pocs and Constantinos Patsakis et al. Backups and the right to be forgotten in the GDPR: An uneasy relationship. In: Computer Law & Security Review. 2018.

[28] Christian Kurtz and Florian Wittner and Martin Semmann and Wolfgang Schulz and Tilo Böhmann et al. Accountability of platform providers for unlawful personal data processing in their ecosystems–A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR. 2022.

[29] Charles D. Raab et al. Information privacy, impact assessment, and the place of ethics. In: Computer Law & Security Review. 2020.

[30] Lopes, Isabel Maria and Guarda, Teresa and Oliveira, Pedro et al. General Data Protection Regulation in Health Clinics. In: J. Med. Syst. 2020.

[31] Dalrymple, H W. The general data protection regulation, the clinical trial regulation and some complex interplay in pediatric clinical trials. In: Eur. J. Pediatr. 2021.

[32] Ondřej Kročil and Richard Pospíšil et al. The influence of GDPR on activities of social enterprises. In: Mob. Netw. Appl. 2020.

[33] Jost, Patrick and Lampert, Marisa et al. Two years after: A scoping review of GDPR effects on SeriousGames research ethics reporting. In: Springer International Publishing. 2020.

[34] Mee, Blanaid and Kirwan, Mary and Clarke, Niamh and Tanaka,Aoife and Manaloto, Lino and Halpin, Emma and Gibbons, Una andCullen, Ann and McGarrigle, Sarah and Connolly, Elisabeth M andBennett, Kathleen and Gaffney, Eoin and Flanagan, Ciaran andTier, Laura and Flavin, Richard and McElvaney, Noel G et al. What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective. In: Ir. J. Med. Sci. 2021.

[35] Gazi, Theodora et al. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. In: J. Int. Humanit. Action. 2020.

[36] de Carvalho, Renata M and Del Prete, Camillo and Martin, Yod et al. Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects. In: SN Computer Science. 2020.

[37] Phillips, Mark et al. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). In: Hum. Genet. 2018.

[38] Roberts L. Multiple Computer Networks and Intercomputer Communication. Washington, 1967.

[39] Internet World Stats [página na internet]. Internet World Stats - Stats [acesso em 05 de fevereiro de 2022]. Disponível em https://www.internetworldstats.com/stats.htm

[40] Marcus A. Data and the fourth industrial revolution. [publicação na web]; 2015 acesso 05 de fevereiro de 2022. Disponível em https://www.weforum.org/agenda/2015/12/data-and-the-fourth-industrial-revolution/

[41] Rifkin J. La era del acceso: La revolución de la nueva economía. Barcelona: Paidós, 2013.

[42] Pentland A. The Data-Driven Society. Revista Scientific American [revista em internet] Outubro de 2013; acesso 06 de fevereiro de 2022. Disponível em https://www.scientificamerican.com/

[43] Brynjolfsson E, Mcafee A. The Second Machine Age: Work, Progress, and Prosperity in a time of Brilliant Technologies. New York: Norton, 2016.

[44] Kuneva M. Roundtable on Online Data Collection, Targeting and Profiling. Brussels, 2009.

[45] General Data Protection Regulation (GDPR) [página na internet]. General Data Protection Regulation (GDPR) [acesso em 08 de fevereiro de 2022]. Disponível em https://gdpr-info.eu/

[46] Piwik PRO Analytics Suite [página na internet]. 10 new privacy laws around the world and how they’ll affect your analytics [acesso em 07 de fevereiro de 2022]. Disponível em https://piwik.pro/privacy-laws-around-globe/

[47] Kitchenham B, Charters S. Guidelines for Performing Systematic Literature Reviews in Software Engineering. Reino Unido, 2007.

[48] Aridor G, Che Y, Salz T. The Economic Consequences Of Data Privacy Regulation: Empirical Evidence From GDPR. Reino Unido, 2020

[49] Haroon MZ, Zeb Z, Javed Z, Awan Z, Aftab Z, Talat W. Internet addiction in medical students. Paquistão, 2018.

[50] Li H, Yu L, He W. The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management [revista em internet] 2019; acesso 07 de fevereiro de 2022. Disponível em https://www.tandfonline.com/

[51] Pinsent Masons [página na internet]. British Airways fined £20m over GDPR breach [acesso em 12 de fevereiro de 2022]. Disponível em https://www.pinsentmasons.com/out-law/news/british-airways-fined-20m-over-gdpr-breach

[52] Information Commissioner's Office (ICO) [página na internet]. ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure [acesso em 12 de fevereiro de 2022]. Disponível em https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

[53] European Commission [página na internet]. Keynote speech by Commissioner Jourová at General Data Protection Regulation conference [acesso em 12 de fevereiro de 2022]. Disponível em https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3949

[54] Sen S, Guha S,Datta A, Rajamani SK, Tsai J, Wing JM. Bootstrapping Privacy Compliance in Big Data Systems. IEEE Symposium on Security and Privacy; 2014.

[55] Startup Guide - IONOS [página na internet]. Compliance: guidelines for compliant corporate behaviour [acesso em 12 de fevereiro de 2022]. Disponível em https://www.ionos.co.uk/startupguide/grow-your-business/compliance/

[56] Teixeira G, Mira da Silva M, Pereira, R. The critical success factors of GDPR implementation - a systematic literature review. Portugal, 2019.

[57] Kutz C, Semmann M, Böhmann T. Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Twenty-fourth Americas Conference on Information Systems, 2018.

[58] Bassani R, Cazella S. O Alinhamento Entre Learning Analytics E A General Data Protection Regulation: Uma Revisão Sistemática De Literatura. Campinas, 2021.

[59] SAP [página na internet]. GDPR: sete princípios fundamentais [acesso em 07 de maio de 2022]. Disponível em https://news.sap.com/brazil/2019/05/gdpr-sete-principios-fundamentais-bl0g/

[60] Robert Feldt and Ana Magazinius et al. Validity Threats in Empirical Software Engineering Research - An Initial Survey. In: ESEM. 2010.

[61] Law Insider [página na internet]. Privacy Law definition [acesso em 07 de maio de 2022]. Disponível em https://www.lawinsider.com/dictionary/privacy-law

[62] Planalto [página na internet]. Lei Geral de Proteção de Dados Pessoais (LGPD). [acesso em 07 de maio de 2022]. Disponível em planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[63] State of California Department of Justice [página na internet]. California Consumer Privacy Act (CCPA). [acesso em 07 de maio de 2022]. Disponível em https://oag.ca.gov/privacy/ccpa

[64] Neotel [página na internet]. CCPA – O Que É A Lei De Privacidade Do Consumidor Da Califórnia?. [acesso em 07 de maio de 2022]. Disponível em https://www.neotel.com.br/blog/2020/08/21/ccpa-o-que-e-a-lei-de-privacidade-do-consumidor-da-california/

[65] Neves, Rebeca et al. GDPR e LGPD: Estudo comparativo. In: Faculdade de Ciências Jurídicas e Sociais - FAJS. 2021.