UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

SISTEMAS DE INFORMAÇÃO

RUAN ALEXSANDER VIEIRA

Um Estudo Sobre a Adequação de Empresas de Saúde às Leis de Privacidade

Recife

2022

RUAN ALEXSANDER VIEIRA

Um Estudo Sobre a Adequação de Empresas de Saúde às Leis de Privacidade

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Jéssyka Vilela

Recife

2022

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Vieira, Ruan Alexsander.
Um estudo sobre a adequação de empresas de saúde às leis de privacidade / Ruan Alexsander Vieira. - Recife, 2022.
42 p.

Orientador(a): Jéssyka Flavyanne Ferreira Vilela
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2022.

1. leis de proteção de dados. 2. dados pessoais. 3. saúde. I. Vilela, Jéssyka Flavyanne Ferreira. (Orientação). II. Título.

000 CDD (22.ed.)

RUAN ALEXSANDER VIEIRA

Um Estudo Sobre a Adequação de Empresas de Saúde às Leis de Privacidade

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data da Defesa do TCC:

Recife, 20 de Outubro de 2022

BANCA EXAMINADORA

_____

Profa. Jéssyka Flavyanne Ferreira Vilela (Orientadora)
UNIVERSIDADE FEDERAL DE PERNAMBUCO

_____

Prof. Vinicius Cardoso Garcia (2º membro da banca)
UNIVERSIDADE FEDERAL DE PERNAMBUCO

_____

Profa. Mariana Maia Peixoto (3º membro da banca)
UNIVERSIDADE FEDERAL DE PERNAMBUCO

AGRADECIMENTOS

Meus sinceros agradecimentos a toda a minha família, a minha namorada, todos os professores do CIn e principalmente a professora Jéssyka que me aguentou e me guiou por essa jornada!

"O importante não é vencer todos os dias, mas lutar sempre." (Waldemar Valle Martins)

RESUMO

A necessidade de adequação às leis de privacidade, como a *General Data Protection Regulation* (GDPR), provocou diversas mudanças nas empresas. Uma área que teve um grande impacto foram as empresas da área de saúde por conta da imensa quantidade de dados sensíveis que manuseiam. Portanto, é importante investigar as medidas de adequação adotadas por esse setor, assim como as dificuldades enfrentadas. Este trabalho objetiva realizar um estudo sistemático da literatura sobre a adequação de empresas da área de saúde às leis de proteção de dados. A partir desse estudo pode-se identificar a GDPR como lei base para estudos na área de adequação a leis de privacidade em empresas de saúde e que há uma concentração na área de atendimento à saúde e pesquisa. Foi identificado também que o maior desafio enfrentado por essas empresas é o na adequação aos princípios básicos e direitos dos titulares ditadas pela GDPR.

Palavras-chave: leis de privacidade, dados pessoais, saúde

ABSTRACT

The need to adapt to privacy laws, such as the General Data Protection Regulation, GDPR, has caused several changes in companies. One area that had a big impact was healthcare companies because of the huge amount of sensitive data they handle. Therefore, it is important to investigate the adequacy measures adopted by this sector, as well as the difficulties faced. This work aims to carry out a systematic study of the literature on the adequacy of healthcare companies to data protection laws. From this study, the GDPR can be identified as the base law for studies in the area of adequacy to privacy laws in health companies and that there is a concentration in the area of healthcare and research. It was also identified that the biggest challenge faced by these companies is in adapting to the basic principles and rights of the data owners dictated by GDPR.

Keywords: privacy law, personal data, health

LISTA DE ILUSTRAÇÕES

Figura 1. Processo de seleção de estudos no snowballing. 18
Figura 2. Ano de publicação dos artigos. 21
Figura 3. Leis de privacidade dos artigos. 27
Figura 4. Tipos de contribuição dos artigos. 28
Figura 5. Área da saúde de atuação dos artigos. 30

LISTA DE TABELAS

Tabela 1. Artigos selecionados para snowballing. 19
Tabela 2. Desafios reportados pelos estudos selecionados. 22
Tabela 3. Boas práticas pelos estudos selecionados. 26
Tabela 4. Mecanismos reportados pelos estudos selecionados. 28
Tabela 5. Impactos das leis reportados pelos estudos selecionados. 31
Tabela 6. Métodos de pesquisa reportados pelos estudos selecionados. 32
Tabela 7. Principais conclusões reportadas pelos estudos selecionados. 34
Tabela 8. Trabalhos futuros reportados pelos estudos selecionados. 36

LISTA DE ABREVIATURAS E SIGLAS

GDPR	*General Data Protection Regulation*
DPD	*Data Protection Directive*
OCR	*Office for Civil Rights*
DPO	*Data Protection Officer*
DPA	*Data Protection Agency*
LGPD	Lei Geral de Proteção de Dados
OECD	*Organization for Economic Co-operation and Development*
WGBO	*Wet geneeskundige behandelingsovereenkomst*
HIPAA	*Health Insurance Portability and Accountability Act*
HSCA	*Health and Social Care Act*
EHRs	*Electronic Health Records*
IA	Inteligência Artificial

SUMÁRIO

1 INTRODUÇÃO 12

1.1 CONTEXTUALIZAÇÃO 12

1.2 MOTIVAÇÃO 12

1.3 OBJETIVOS 13

1.3.1 Pergunta de Pesquisa 13

1.3.2 Objetivo 13

1.4 ESTRUTURA DE TRABALHO 13

2 REFERENCIAL TEÓRICO 14

2.1 Leis de Privacidade 14

2.2 GDPR 14

2.3 Bases Legais na GDPR 15

2.4 Direitos do Titular na GDPR 15

2.5 Princípios da GDPR 16

2.6 Dados Pessoais 17

3 METODOLOGIA 18

3.1 Seleção dos artigos iniciais 18

3.2 Critérios de Inclusão e Exclusão 19

3.3 Perguntas de Pesquisa 20

3.4 Ameaças à validade 20

4 Resultados 21

4.1 Ano de publicação dos estudos selecionados 21

4.2 Quais são os desafios enfrentados por empresas de saúde para adequação às leis de privacidade? 22

4.3 Quais são as boas práticas utilizadas por empresas de saúde para adequação às leis de privacidade? 26

4.4 Qual (is) lei(s) de privacidade são mencionadas nos estudos selecionados? 27

4.5 Qual o tipo de contribuição dos estudos selecionados? 27

4.6 Qual a área de atuação dentro do contexto da saúde mencionada no estudo? 30

4.7 Qual(is) impactos das leis de privacidade nas empresas de saúde? 31

4.8 Qual o método de pesquisa utilizado nos estudos selecionados? 32

4.9 Quais são as principais conclusões a que os artigos obtiveram? 34

4.10 Quais são as sugestões para os trabalhos futuros mencionadas nos estudos? 36

4.11 Discussão dos resultados 37
5 CONCLUSÃO 39
5.1 Trabalhos Futuros 39
REFERÊNCIAS 40

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

Todo ano milhares de pessoas procuram atendimento de saúde e pesquisas na área são desenvolvidas com o intuito de melhorar a qualidade de vida e descobrir novos tratamentos para doenças. Com o advento da tecnologia o uso de sistemas eletrônicos para facilitar o trabalho dos profissionais de saúde vem aumentando e se desenvolvendo constantemente.
Esses sistemas costumam guardar dados pessoais dos pacientes, que sozinhos ou em conjunto com outros dados podem vir a identificá-los e até mesmo conter dados sensíveis, esses que podem vir a acarretar em discriminação ao titular, esse tema é discutido com mais detalhes na sessão 2.6. Todavia, ataques a esses sistemas e vazamentos ocorrem constantemente [1].

Em novembro de 2015, a empresa *Excellus BlueCross BlueShield* reconheceu um ataque em que houve o vazamento de 10 milhões de dados de pacientes. Essa empresa foi condenada em corte a pagar um valor de 5.1 milhões de dólares em multa à *Office for Civil Rights* (OCR)[32]. Vazamentos como esse reforçam a necessidade de investimento em segurança de informação, treinamento e adoção de procedimentos mais rigorosos para evitar vazamentos dos dados dos pacientes.
Nesse contexto, tem havido um desenvolvimento e atualização de leis de proteção de dados pelo mundo para que também haja uma abrangência a esses sistemas, como também ao meio analógico, impulsionado principalmente pela *General Data Protection Regulation* (GDPR), lei de proteção de dados europeia. Dito isso, há uma necessidade de adequação por parte das empresas para garantir a segurança e privacidade e os direitos dos usuários sob os seus dados.
Porém, mesmo com o surgimento e atualização dessas leis, os ataques e vazamentos não param. Apenas em Janeiro de 2021 na Espanha, o setor de saúde sofreu em média 626 ataques por semana por empresa [31]. Por isso a não conformidade a essas leis pode acarretar em multa que pode chegar a 17 milhões de euros ou 4% da receita anual da empresa [33].
Sendo assim, a necessidade de adequação e investimento em privacidade e segurança da informação se tornou necessária para a sobrevivência das empresas de saúde. Para isso é interessante o estudo dos desafios enfrentados, boas práticas, mecanismos adotados pelas empresas que já se adequaram, a fim de ter um norte e facilitar a adequação de futuras empresas que desejam atuar na área.

1.2 MOTIVAÇÃO

As informações manipuladas por empresas de saúde são, em sua maioria, dados pessoais sensíveis, que são dados que podem levar a discriminação do titular, como dados biométricos e histórico médico. Essas informações possuem alto grau de criticidade e, portanto, requerem um alto grau de proteção dos dados.

A motivação deste trabalho é investigar os desafios, aprender as boas práticas, os possíveis mecanismos e os impactos das leis de privacidade que possam ajudar na adequação a leis de proteção de dados, com o objetivo de identificar os pontos citados acima.
Foi escolhida uma revisão sistemática pois assim não haveria necessidade de marcar reuniões com os gestores de empresas da área e realizar entrevistas, pois isso consumiria muito tempo e o tempo para a realização do estudo era limitado por se tratar de um trabalho de graduação. A GDPR foi a lei escolhida como base por conta da quantidade de estudos que já foram realizados com ela como base.

1.3 OBJETIVOS

1.3.1 Pergunta de Pesquisa

A pergunta de pesquisa para esse trabalho é: Como têm ocorrido a adequação de empresas de saúde às leis de proteção de dados?

1.3.2 Objetivo

O objetivo geral deste trabalho é investigar o contexto de adequação das empresas da área de saúde às leis de privacidade. Como objetivos específicos, destacam-se: (1) Realizar uma revisão sistemática da literatura sobre adequação de empresas de saúde as leis de proteção de dados; (2) Identificar os desafios reportados pela literatura para a adequação; (3) Catalogar boas práticas e procedimentos e técnicas utilizadas para atingir a conformidade de forma a auxiliar a adequação futura de empresas do mesmo ramo.

1.4 ESTRUTURA DE TRABALHO

Este trabalho está organizado da seguinte forma:
● Capítulo 1 – Introdução: Neste capítulo é apresentado uma introdução sobre o tema escolhido e sua importância, contendo uma contextualização, motivo e objetivos de pesquisa.
● Capítulo 2 – Referencial Teórico: Neste capítulo é apresentado o referencial teórico sobre as leis de privacidade e a GDPR, lei escolhida como base para o estudo.
● Capítulo 3 – Metodologia: Neste capítulo é apresentado a metodologia utilizada para a realização deste artigo.
● Capítulo 4 – Resultados: Neste capítulo são apresentados os resultados coletados dos artigos selecionados após a aplicação da metodologia escolhida.
● Capítulo 5 – Conclusão: Neste capítulo é apresentado a conclusão a que foi chegada e sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Nessa seção são apresentados os conceitos básicos sobre leis de proteção de dados, GDPR, base legal, direitos dos titulares, os princípios de tratamento de dados e definição de dados pessoais e sensíveis.

2.1 LEIS DE PRIVACIDADE

As leis de privacidade são conjuntos de leis que buscam garantir a privacidade e segurança dos dados pessoais das pessoas. Para garantir o seu cumprimento, as leis de privacidade possuem princípios a serem seguidos e punições em casos de não conformidade.

Para ser considerada uma lei de um país ser considerada uma lei de privacidade de dados, ela precisa especificar um conjunto básico de princípios de privacidade de dados, com um padrão mínimo previsto pelas diretrizes da *Organisation for Economic Co-operation and Development* (OECD), ou do *Council of Europe Convention 108* [34]. É necessário também não ser autorregulatória e ter órgão regulador oficial do estado para garantir a adequação e cumprimento [34].

A primeira lei de privacidade nacional de que se têm registro é a *Data Act*, de 1973, da Suécia, e foi também a primeira a implementar esses conjuntos básicos de princípios [34]. Nesses 49 anos desde a criação da *Data Act*, diversos outros países e uniões econômicas e políticas, como a União Europeia, com a *Data Protection Directive* (DPD) e mais recentemente a GDPR, lei que veio para a substituir [1], desenvolveram seus próprios conjuntos de leis.

2.2 GDPR

A GDPR, lei aprovada em 14 de Abril de 2016 e que entrou em vigor em 25 de Maio de 2018, é a lei desenvolvida pela Comissão Europeia para ser a sucessora, com o intuito de possuir um escopo maior que a DPD, lei de 1995 [1]. Ambas as leis regulam o processamento e compartilhamento dos dados pessoais, possibilitando aos titulares dos dados, a partir de autorização, edição e solicitação de deleção, controle e acesso sob os mesmos.

A principal diferença entre essas leis é a abrangência, visto que a DPD era válida apenas para os estados membros da União Europeia, enquanto a GDPR abrange também estados não membros. Dito isso, mesmo empresas não europeias que atuam no continente devem seguir as normas estabelecidas pela GDPR.

Visando garantir o cumprimento da lei e evitar multas, a GDPR informa que faz-se necessário nas empresas um setor voltado para a adequação da lei. O responsável pelo setor, o *Data Protection Officer* (DPO), é responsável por manter a adequação da empresa, monitorar os processos específicos e colaborar com a autoridade supervisionadora. Do lado do estado, a GDPR faz necessário a criação do *Data Protection Agency* (DPA), que é um órgão cuja responsabilidade é lidar com as queixas dos titulares quanto a não conformidade das empresas à lei [33].

2.3 Bases Legais na GDPR

A GDPR apresenta seis bases legais as quais os dados dos titulares podem ser coletados e processados, sendo eles o consentimento, contrato, a obrigação legal, os interesses vitais, as tarefas públicas e os interesses legítimos definidos a seguir [33].

- **Consentimento:** As empresas de saúde devem obter o consentimento do titular para que os dados possam ser coletados e processados. Essa ação deve ser deliberada por parte do titular [33].
- **Contrato:** Quando firmado um contrato com o titular, os dados podem ser coletados e processados com a finalidade do cumprimento deste contrato [33].
- **Obrigações legais:** Nessa base legal, é permitido a coleta e processamento dos dados do titular quando há a necessidade para estar em conformidade com a lei [33].
- **Interesses vitais:** É considerado de interesse vital, quando a coleta e processamento dos dados do titular têm a finalidade de garantir segurança ou em casos de emergência [33].
- **Tarefas públicas:** É respaldado pela GDPR a coleta e processamento dos dados do titular, quando há a necessidade para interesses públicos e sociais [33].
- **Interesses legítimos:** E por fim, é permitida a coleta e processamento dos dados do titular quando apresentado interesse legítimo, como por exemplo na área de pesquisa voltada para saúde que é utilizado para desenvolvimento de novos tratamentos ou estudos de doenças [33].

2.4 Direitos do Titular na GDPR

Os direitos que os titulares possuem perante à GDPR são oito, sendo eles o direito de ser informado, o direito a acesso, o direito a retificação/correção, o direito a deleção, o direito à restrição de processamento, o direito à portabilidade dos dados, o direito de contestar e o direito de não ser objeto de decisões automatizadas definidos a seguir [33].

- **Direito de Ser Informado:** O titular dos dados tem o direito a saber como as empresas coletam e usam seus dados pessoais, por quanto tempo pretendem armazenar os seus dados e também com quem esses dados serão compartilhados [33]. As empresas que fazem a coleta também precisam informar os nomes e contatos das empresas com quem esses dados serão compartilhados [33].
- **Direito a Acesso:** Perante à GDPR, o titular possui o direito de ter acesso a todos os seus dados que estão em posse da empresa que coletou, e o que pretende fazer com os mesmos [33].
- **Direito a Correção:** Com o acesso aos dados coletados pelas empresas, o titular pode verificar a integridade dos seus dados e com isso solicitar correção caso necessário ou até mesmo em alguns casos ele mesmo corrigir [33].
- **Direito a Deleção:** O titular dos dados tem o direito a solicitar a deleção de todos os seus dados [33]. Porém, caso seus dados sejam necessários para algo maior que o indivíduo, como em casos de segurança e saúde pública, seus dados não poderão ser deletados imediatamente [33].

- **Direito a Restrição de Processamento:** Caso os dados do titular não possam ser deletados imediatamente, o mesmo tem o direito de solicitar uma restrição de processamento, fazendo assim com que seus dados sejam usados apenas para necessidades sociais [33].
- **Direito à Portabilidade dos Dados:** O titular dos dados tem direito a solicitar a qualquer momento a portabilidade de todos os seus dados para serem reutilizados em qualquer outro serviço/empresa da sua escolha [33]. Essa portabilidade pode ser feita diretamente para o titular ou para serviço que o mesmo tenha escolhido [33].
- **Direito de Contestar:** O titular tem o direito de contestar o processamento de seus dados caso seus dados estejam sendo utilizados por empresas para realizar marketing direto, para pesquisas ou para fins sociais [33]. Porém essas empresas podem continuar o processamento desses dados caso consigam provar que há a necessidade de usá-los para fins que sobreponham o direito individual [33].
- **Direito de Não Ser Objeto de Decisões Automatizadas:** O titular tem o direito de solicitar intervenção humana caso os seus dados estejam sendo utilizados por algoritmos para decisões automatizadas [33]. As empresas têm o dever de informar se esses dados serão objeto de decisões automatizadas de antemão, dando assim a possibilidade ao titular de negar a utilização de seus dados para essa finalidade [33].

2.5 Princípios da GDPR

A GDPR possui sete princípios a que as empresas devem seguir, sendo elas a legalidade, justiça e transparência, limitação de propósito, minimização dos dados, precisão, limitação de armazenamento, integridade e confidencialidade e responsabilidade [33].

- **Legalidade, Justiça e Transparência:** Esses três termos juntos formam o primeiro princípio a qual a empresa precisa seguir, que é ter um motivo justo para coletar os dados, sendo por consentimento do titular, cumprir com medidas legais, questões contratuais, proteger interesse vital do titular, por questões de interesse social ou provando interesse legítimo que não sobreponha os direitos do titular [33]. Ela também diz que as empresas não podem esconder o real motivo da coleta ou processamento e precisam ser claros e honestos sobre quem são, para que e como estão utilizando os dados dos titulares [33].
- **Limitação de Propósito:** Esse princípio diz que as empresas só podem utilizar os dados coletados para atividades específicas, sendo essas atividades explicitadas, específicas e para propósitos legítimos, ao titular [33]. Caso seja necessário, o uso desses dados para novas atividades, deve ser necessário uma nova solicitação de consentimento ao titular, salvo em casos referentes a obrigações perante a lei [33].
- **Minimização dos Dados:** Nesse terceiro princípios, a GDPR diz que os dados coletados devem ser mantidos o mínimo possível para a conclusão do propósito específico [33].
- **Precisão:** Esse princípio explicita que é de responsabilidade da empresa que coletou os dados garantir a precisão dos dados, realizando vistorias, melhorias e exclusão dos dados incorretos ou incompletos [33].

- **Limitação de Armazenamento:** Nesse princípio, a GDPR afirma que as empresas são responsáveis por informar por quanto tempo ficarão com os dados, sendo necessário após a passagem desse tempo a anonimização para que não sejam mais utilizados [33].
- **Integridade e Confidencialidade:** Esse princípio diz que é de responsabilidade da empresa que coletou os dados garantir a integridade e confidencialidade dos mesmos, mantendo-os seguros de ameaças internas e externas [33].
- **Responsabilidade:** Esse último princípio diz respeito a empresa manter com a palavra de que está os princípios propostos pela GDPR. Para isso, é necessário a documentação das decisões e atividades realizadas para caso da necessidade de realização de uma auditoria a fim de provar a responsabilidade [33].

2.6 Dados Pessoais

Para a GDPR, dados pessoais são todo e qualquer dado que possa vir a identificar o titular, até mesmo aqueles dados que separados podem não identificar ninguém, mas em um conjunto de dados podem vir a identificar, como peso, altura, idade [33]. Porém, dentro desses dados existe uma categoria de dados considerados sensíveis, que precisam de um grau maior de proteção, pois são dados que se vasados podem levar a discriminação do titular, são exemplos de dados sensiveis dados, sobre raça, etnia, alinhamento político, crenças, religiosa, espirituais ou filosoficas, dado biométrico, dados sobre saúde, vida e orientação sexual e dados genéticos [33].

3 METODOLOGIA

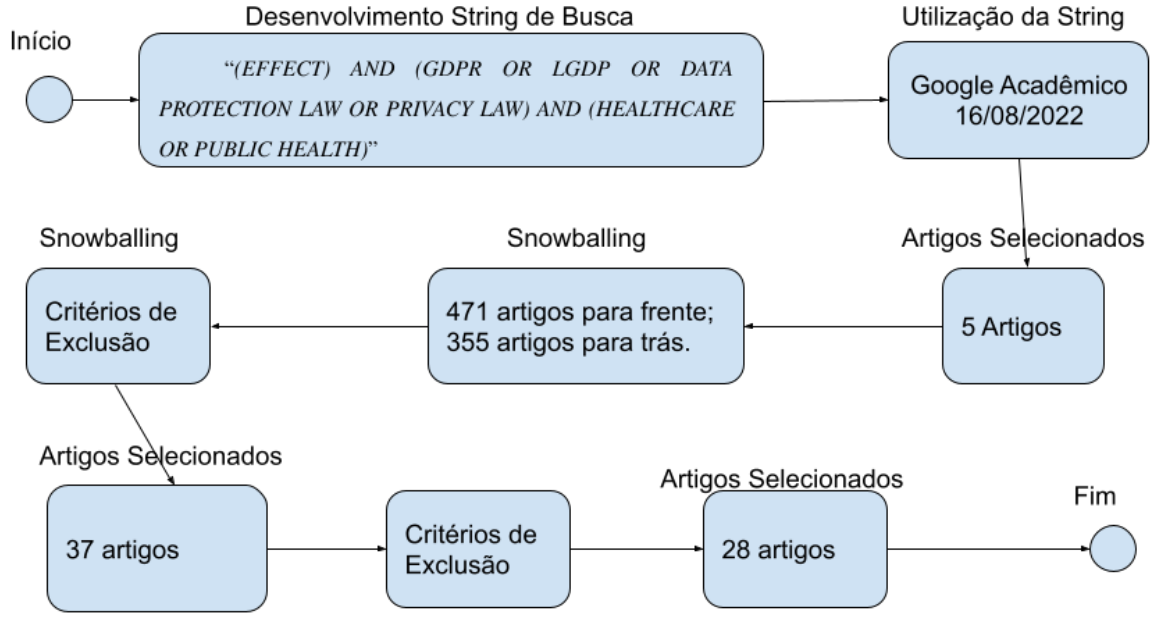
A metodologia adotada para executar esse trabalho consistiu de duas etapas:

1. **Revisão de literatura**: foram investigados conceitos de privacidade, leis de privacidade e GDPR descritos no capítulo 2;

2. **Snowballing**: a partir de um conjunto inicial de estudos, foram identificados novos trabalhos que abordam avaliação de políticas de privacidade;

A técnica utilizada para executar o estudo sistemático foi *snowballing* [30] que consiste no uso da lista de referências de um artigo (*backward*) ou as citações deste artigo (forward) para identificar trabalhos adicionais a fim de identificar os desafios enfrentados, as boas práticas adotadas, a lei a que houve a adequação, a possível contribuição caso tenham desenvolvido novos métodos e a área de atuação dentro da área de saúde. A Figura 1 resume os passos adotados na realização deste trabalho.

Figura 1. Processo de seleção de estudos no snowballing.



Fonte: O autor (2022).

3.1 SELEÇÃO DOS ARTIGOS INICIAIS

Para aplicar a técnica snowballing, primeiro é necessário identificar um conjunto primário de artigos a serem usados como ponto de partida. Para este trabalho, foi utilizado o *Google Scholar* para selecionar 5 artigos, dessa forma, é evitado viés na seleção dos trabalhos. Foi desenvolvido

uma string de busca composta por palavras chaves voltadas ao assunto, sendo utilizada a string "*(EFFECT) AND (GDPR OR LGDP OR DATA PROTECTION LAW OR PRIVACY LAW) AND (HEALTHCARE OR PUBLIC HEALTH)*" que foi utilizada no dia 16 de Agosto de 2022.
A partir dos 6 artigos selecionados, listados na Tabela 1, foram identificados 471 artigos para realizar snowballing para frente e 355 para realizar para trás, representando no total 826 artigos que foram catalogados para a utilização da técnica.

Tabela 1. Artigos selecionados para snowballing.

Título	**Ano**	**Quantidade de referências**	**Quantidade de citações**
The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A Case Study [1]	2018	28	2
Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A Case Study in a Portuguese Healthcare Organization [2]	2020	22	0
Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach [3]	2016	70	130
The impact of the EU general data protection regulation on scientific research [4]	2017	13	146
An exhaustive survey on security and privacy issues in Healthcare 4.0 [5]	2020	150	182
The risk-based approach under the new EU data protection regulation: a critical perspective [6]	2019	72	11
Total		355	471

3.2 Critérios de Inclusão e Exclusão

Os critérios de exclusão utilizados foram: o ano dos artigos, não podendo ser mais antigo que 2016, ano em que GDPR foi aprovada como lei, estar nas línguas inglesa ou portuguesa, não ser literatura cinza e fazer uma avaliação das consequências das leis de privacidade sobre as empresas da área de saúde.
Na primeira aplicação do critério de exclusão foram lidos o título, o resumo, a introdução e a conclusão, com o intuito de verificar se os artigos selecionados no *snowballing* faziam avaliação

das consequências das leis de privacidade sobre as empresas da área de saúde. Com isso foram excluídos 789 artigos.
A utilização da técnica de *snowballing* se iniciou no dia 18 de Agosto de 2022 e foi finalizada no dia 07 de Setembro de 2022.

3.3 Perguntas de Pesquisa

No total foram selecionados 37 artigos, dos quais esses foram submetidos a mais critérios de exclusão onde, a partir da leitura completa seria observado se respondia às seguintes perguntas de pesquisa:

- Quais são os desafios enfrentados por empresas de saúde para adequação às leis de privacidade?
- Quais são as boas práticas utilizadas por empresas de saúde para adequação às leis de privacidade?
- Qual (is) lei(s) de privacidade são mencionadas nos estudos selecionados?
- Qual o tipo de contribuição dos estudos selecionados?
- Qual a área de atuação dentro do contexto da saúde mencionada no estudo?
- Qual(is) impactos das leis de privacidade nas empresas de saúde?
- Qual o método de pesquisa utilizado nos estudos selecionados?
- Quais são as principais conclusões a que os artigos obtiveram?
- Quais são as sugestões para os trabalhos futuros mencionadas nos estudos?

A partir dos 37 trabalhos selecionados previamente, foram selecionados 28 artigos aos quais foram extraídos os dados referentes às perguntas de pesquisa apresentadas neste trabalho. Nesse último passo foram excluídos mais 9 artigos com base nesses critérios de exclusão. No total foram excluídos 798 artigos nas duas aplicações do critério de exclusão.

3.4 Ameaças à validade

Para reduzir ameaças à validade dessa pesquisa, os trabalhos selecionados são publicados em conferências e periódicos de alta qualidade [29]. Esses artigos também apresentam uma grande quantidade de citações, o que sugere a relevância deles para o estudo. Os artigos iniciais também foram publicados em diferentes comunidades científicas com o objetivo de aumentar a variedade entre os trabalhos selecionados [29].

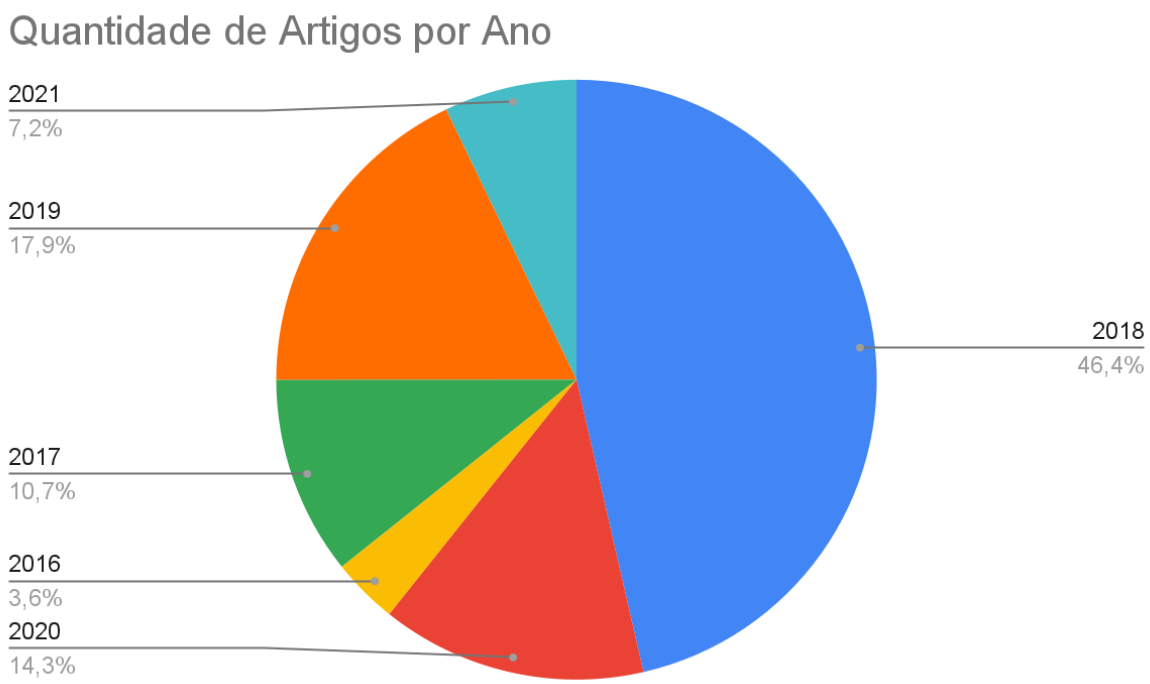
4 RESULTADOS

Nas próximas seções são apresentados os resultados extraídos a partir dos estudos selecionados.

4.1 ANO DE PUBLICAÇÃO DOS ESTUDOS SELECIONADOS

Ao analisar o ano de publicação dos estudos selecionados, foi possível observar a variação da quantidade de artigos sobre o tema durante os anos. A partir da Figura 2, observa-se que houve um aumento da quantidade de pesquisas de 2016, ano em que a lei foi aprovada, até o pico em 2018, ano em que a GDPR entrou em vigor, e logo em seguida uma diminuição. Esse comportamento pode ser explicado pelo fato de não haver punições legais nesses dois 2 primeiros anos após aprovação da lei, por ter sido o tempo dado para adequação. Porém em 2018 com a entrada em vigor, a preocupação com punições fez com que houvesse um maior cuidado a entender e se adequar corretamente a lei para que não houvesse consequências legais.

Figura 2. Ano de publicação dos artigos.



Fonte: O autor (2022).

Após esse pico é possível observar uma diminuição de pesquisas relacionadas à lei pois já há uma maior a habituação e exemplos a serem seguidos das empresas que conseguiram se adequar corretamente. Porém, como as leis são orgânicas e sofrem modificações para acompanharem os avanços tecnológicos e da sociedade, pode-se prever que a cada atualização da lei haverá um

novo pico de estudos para tentar decifrar as boas práticas e melhores ferramentas para adequação.

4.2 QUAIS SÃO OS DESAFIOS ENFRENTADOS POR EMPRESAS DE SAÚDE PARA ADEQUAÇÃO ÀS LEIS DE PRIVACIDADE?

A partir do levantamento dos desafios enfrentados pelas empresas de saúde a adequação a GDPR, foi possível observar que há uma maior dificuldade ao cumprimento dos princípios e direitos básicos dos titulares [3][5][6][8][10][11][12][13][14][18][19][20][22][24][25][26][28], sendo citados como desafio por 17 estudos, dentre elas sendo a principal, e que mais se destacou, o princípio do consentimento [3][10][11][13][14][22][24][25][28], sendo citado 9 estudos.
Isso ocorre por conta de uma maior conscientização dos pacientes quanto aos seus direitos perante a GDPR [1], e por conta da necessidade de uma grande base de dados por parte das empresas com foco em pesquisa científica [3][10][13][22][24][25][28], sendo citados como desafio por 7 estudos, ao qual solicitar consentimento de todos os titulares se torna extremamente trabalhoso.
Os desafios apresentados pelos estudos selecionados são listados na Tabela 2.

Tabela 2. Desafios reportados pelos estudos selecionados.

Desafio	Referência
Financiamento de novas estruturas	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A estudo de caso [1]
Treinamento da equipe de saúde	
Financiamento de novas estruturas	Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A estudo de caso in a Portuguese Healthcare Organization [2]
Sistemas legado	
Equipe pequena	
Falta de logs nos sistemas	
Analisar os logs existentes	
Consentimento	Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach [3]
Privacidade	An exhaustive survey on security and privacy issues in Healthcare 4.0 [5]
Segurança dos dados	
Confidencialidade	
Integridade	
Propriedade dos dados	

Uso secundário de dados pessoais	
Transparência	The risk-based approach under the new EU data protection regulation: a critical perspective [6]
Processamento de dados	
Uso secundário de dados pessoais	
Financiamento de novas estruturas	2018 Global health care outlook: The evolution of smart health care [7]
Ambiente onipresente	A design of patients data transparency in electronic health records. [8]
Complexidade dos dados	
Privacidade	
Segurança dos dados	
Roubo de identidade e falsificação de dados	Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. [9]
Propriedade e gerenciamento dos dados de saúde armazenados	
Acesso dos empregadores a informações sobre saúde e risco de estigmatização	
Acesso das seguradoras privadas às informações de saúde	
Barreiras para a implementação de *Electronic Health Records* (EHRs) nas clínicas e práticas	
Falta de padronização nos EHRs	
Consentimento	The effect of the general data protection regulation on medical research. [10]
Leis contradizentes	
Conhecimento dos requisitos da GDPR	EU General Data Protection Regulation: Changes and implications for personal data collecting companies. [11]
Privacidade de dados	
Harmonização	
Notificação rápida sobre vazamento de dados	
Designar DPO	
Consentimento	
Portabilidade de dados	
Documentação	
Divulgação de informação	Health information privacy concerns, antecedents, and information disclosure intention in online health communities. [12]
Pseudo anonimização	Rules for processing genetic data for research

Consentimento	purposes in view of the new EU General Data Protection Regulation [13]
Harmonização	
Consentimento	Ethical issues for direct-to-consumer digital psychotherapy apps: addressing accountability, data protection, and consent [14]
Segurança dos dados	
Responsabilidade	
Inteligência artificial (IA) e *machine learning*	Healthcare informatics and privacy [15]
Anonimização	
Segurança dos dados	
Cumprimento oneroso	Big genetic data and its big data protection challenges [17]
Facilitar os direitos do titular dos dados	
Necessidade de obter aprovação ética	
Pseudo anonimização	The EU General Data Protection Regulation: How will it impact the regulation of research biobanks? Setting the legal frame in the Mediterranean and Eastern European área [18]
Uso secundário de dados pessoais	
Extração massiva de dados	Moral bureaucracies and social network research [19]
Processamento de dados	
Perfilização dos dados	
Mau uso de informações médicas, como por exemplo para pesquisa	OpenEHR and general data protection regulation: evaluation of principles and requirements [20]
Falta de treinamento apropria à GDPR	Does GDPR harm or benefit research participants? An EORTC point of view [21]
Interpretação exagerada	
Consentimento	Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR [22]
Portabilidade de dados	Future of data analytics in the era of the general data protection regulation in Europe [24]
Deleção de dados	
Consentimento	
Processamento de dados	
Cooperação entre governo e empresas	Building trust and transparency? Challenges of the opt-out system and the secondary use of health data in England [25]
Consentimento	
Anonimização	
Uso secundário de dados pessoais	

Confidencialidade	Security and Privacy in the Era of Electronic Health Records (EHRs) [26]
Controle de acesso	
Proteção	
Transparência	Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation [28]
Processamento de dados	
Consentimento	
Uso de dados públicos	
Anonimização	
Portabilidade de dados	

4.3 QUAIS SÃO AS BOAS PRÁTICAS UTILIZADAS POR EMPRESAS DE SAÚDE PARA ADEQUAÇÃO ÀS LEIS DE PRIVACIDADE?

A partir do estudo realizado, é possível observar na tabela 3, que existem diversas boas práticas que podem ser adotadas para a adequação a GDPR, mas a boa prática que mais se destacou e que mais foi citada pelos artigos selecionados é o investimento de tempo e capital financeiro [1][11], fazendo assim com que a adequação se torne mais fluida e gerando menos dores de cabeça. As boas práticas listadas nos estudos selecionados são apresentadas na Tabela 3.

Tabela 3. Boas práticas pelos estudos selecionados.

Boas Práticas	**Referência**
Investimento de tempo e capital financeiro	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A Case Study [1], Does GDPR harm or benefit research participants? An EORTC point of view [21]
Consentimento e anonimização	Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach [3]
Uso de logs	A design of patients data transparency in electronic health records. [8]
Investimento em equipe, tempo e capital financeiro	EU General Data Protection Regulation: Changes and implications for personal data collecting companies. [11]
Identificação dupla	Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR [22]
Acesso liberado ao titular dos dados	Security and Privacy in the Era of Electronic Health Records (EHRs) [26]

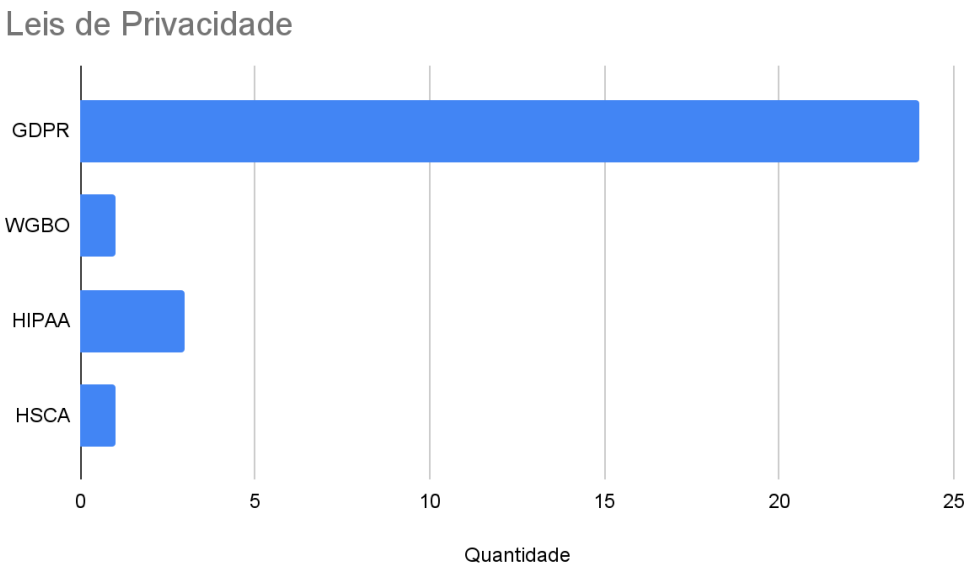
4.4 QUAL (IS) LEI(S) DE PRIVACIDADE SÃO MENCIONADAS NOS ESTUDOS SELECIONADOS?

Ao observar a figura 3, gerada a partir do estudo dos artigos selecionados, é possível notar que a lei de proteção de dados mais estudada é a GDPR. Este resultado é de certa forma esperado visto que sua abrangência é internacional e é necessária segui-la para que as empresas possam atuar no continente europeu. Por conta disso, a GDPR também serviu de base para o desenvolvimento de leis de privacidade em diversos outros países pelo mundo, como a Lei Geral de Proteção de Dados (LGPD), no Brasil.

As demais leis citadas nos estudos selecionados foram *Wet geneeskundige behandelingsovereenkomst* (WGBO), lei holandesa de contrato médico, que diz respeito à segurança e privacidade na área de saúde, a *Health Insurance Portability and Accountability Act* (HIPAA), lei federal estadunidense sancionada em agosto de 1996 e a *Health and Social Care Act* (HSCA), lei britânica sancionada em 2012.

As leis de privacidade mencionadas nos estudos selecionados são listadas na Figura 3.

Figura 3. Leis de privacidade dos artigos.



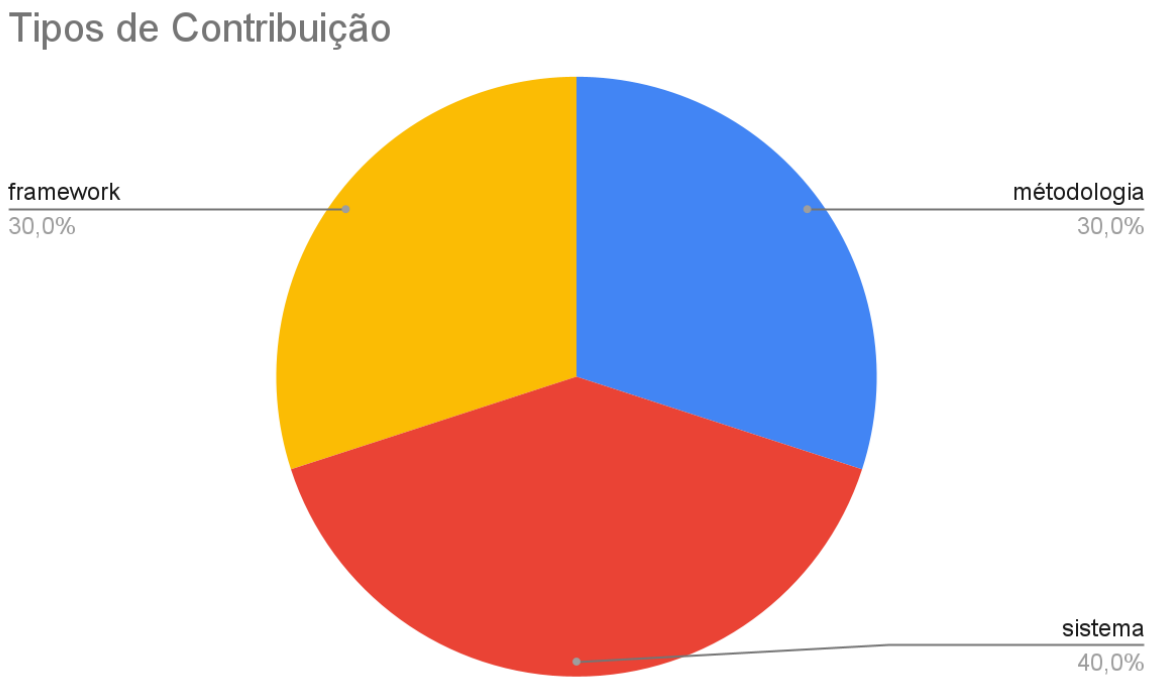
Fonte: O autor (2022).

4.5 QUAL O TIPO DE CONTRIBUIÇÃO DOS ESTUDOS SELECIONADOS?

A partir do estudo foi possível identificar, a partir da figura 4, quais os tipos de mecanismos mais utilizados e recomendados pelos estudos foram o sistemas de informação [2] [3][12][20],

seguido das metodologias [1] [6][26] e frameworks [8] [11][12]. Essas categorias de tipos de contribuição foram definidas a partir das próprias nomenclaturas utilizadas nos estudos.

Figura 4. Tipos de contribuição dos artigos.



Fonte: O autor (2022).

Não foi possível identificar um mecanismo específico que foi mais utilizado, visto que pela tabela 4, é possível observar que os artigos abordam mecanismos distintos, que por diversos motivos vem a se adequar melhor a realidade das empresas estudadas.

Tabela 4. Mecanismos reportados pelos estudos selecionados.

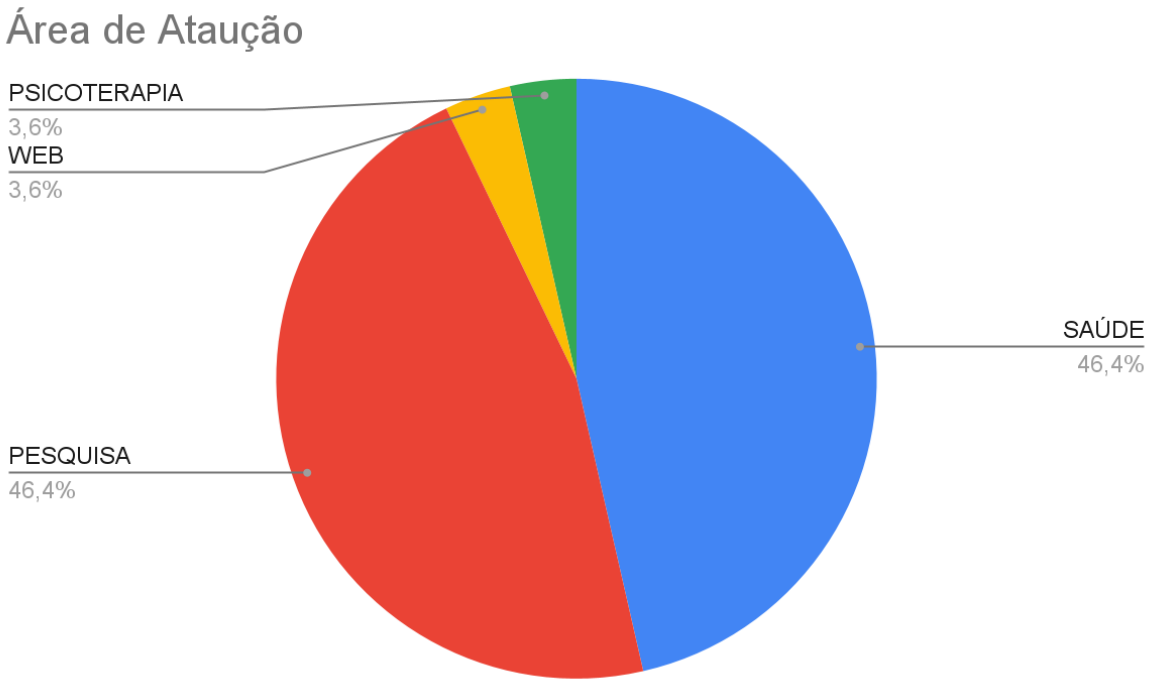
Contribuição	Tipo de Contribuição	Referência
Privacy Calculus	Metodologia	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A estudo de caso [1]
Audit Log	Sistema	Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A estudo de caso in a Portuguese Healthcare

		Organization [2]
Não Informado	Sistema	An exhaustive survey on security and privacy issues in Healthcare 4.0 [5]
Risk-based Approach	Metodologia	The risk-based approach under the new EU data protection regulation: a critical perspective [6]
Framework de Transparência de Dados em Nuvem	Framework	A design of patients data transparency in electronic health records. [8]
Digital Single Market	Sistema	The effect of the general data protection regulation on medical research. [12]
Não Informado	Framework	EU General Data Protection Regulation: Changes and implications for personal data collecting companies. [11]
Dual Calculus e Teoris de Motivação a Proteção	Framework	Health information privacy concerns, antecedents, and information disclosure intention in online health communities. [12]
OpenEHR	Sistema	OpenEHR and general data protection regulation: evaluation of principles and requirements [20]
Encriptação	Metodologia	Security and Privacy in the Era of Electronic Health Records (EHRs) [26]
Assinatura Digital		
Verificação		

4.6 QUAL A ÁREA DE ATUAÇÃO DENTRO DO CONTEXTO DA SAÚDE MENCIONADA NO ESTUDO?

Como a área de saúde possui diversas áreas de atuação, também foi pesquisado a que área esses estudos se baseiam, e como observado na figura 5 é possível ver que a área onde se houve uma maior preocupação de pesquisa foi a de cuidado médico seguida pela área de pesquisa. Isso se dá pelo fato dos hospitais e clínicas serem um dos maiores coletores de dados pessoais e sensíveis, por conta da necessidade de tratamento médico da população.

Figura 5. Área da saúde de atuação dos artigos.



Fonte: O autor (2022).

Já a área de pesquisa apresenta uma grande quantidade por conta da quantidade de dados pessoais e sensível que são necessários para o processamento com a finalidade de realização de pesquisas para desenvolvimento de novos métodos de tratamentos e prevenção de doenças, e até mesmo desenvolvimentos de vacinas para o combate de patógenos, como o vírus da COVID-19, causador da mais recente pandemia global.

4.7 QUAL(IS) IMPACTOS DAS LEIS DE PRIVACIDADE NAS EMPRESAS DE SAÚDE?

O impacto da GDPR mais observado pelos estudos foi de os estados membros da União Europeia poderem fazer derrogações à lei [22] [25][26]. Isso quer dizer que esses estados podem fazer revogações parciais com a finalidade de que a GDPR e as leis locais consigam coexistir, sem que haja conflitos entre elas, e até mesmo se completarem a fim de garantir um conjunto de princípios com o objetivo uma proteção dos dados mais completa e eficaz.
Os impactos listados nos estudos selecionados são apresentados na Tabela 5.

Tabela 5. Impactos das leis reportados pelos estudos selecionados.

Impacto	Referência
Pacientes cientes dos seus direitos	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A Case Study [1]
Atraso no tratamento	
Mais tempo para otimização do tratamento	
Harmonização entre as leis com GDPR	The effect of the general data protection regulation on medical research. [12]
Proteção dos dados por padrão e design	EU General Data Protection Regulation: Change-s and implications for personal data collecting companies. [11]
Processos para lidar com vazamentos de dados postos em prática	
elucidação do termo pseudo anonimização	Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation [13]
amigável à pesquisa sob circunstâncias	Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation [13]
dados genéticos agora são dados sensíveis	Big genetic data and its big data protection challenges [17]
paciente relutantes em conceder dados pessoais	Moral bureaucracies and social network research [19]
estados membros podem fazer derrogações	Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR [22], Building trust and transparency? Challenges of the opt-out system and the secondary use of health data in England [25], Security and Privacy in the Era of Electronic Health

	Records (EHRs) [26]

4.8 QUAL O MÉTODO DE PESQUISA UTILIZADO NOS ESTUDOS SELECIONADOS?

Tabela 6. Métodos de pesquisa reportados pelos estudos selecionados.

Método de Pesquisa	**Referência**
Estudo de Caso	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A estudo de caso [1]
Estudo de Caso	Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A estudo de caso in a Portuguese Healthcare Organization [2]
Revisão	Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach [3]
Visão Global	The impact of the EU general data protection regulation on scientific research [4]
Pesquisa com entrevista	An exhaustive survey on security and privacy issues in Healthcare 4.0 [5]
Não Informado	The risk-based approach under the new EU data protection regulation: a critical perspective [6]
Não Informado	2018 Global health care outlook: The evolution of smart health care [7]
Proposta	A design of patients data transparency in electronic health records. [8]
Pesquisa com entrevista	Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. [9]
Análise de Requisitos	The effect of the general data protection regulation on medical research. [10]
Análise Sistemática	EU General Data Protection Regulation: Changes and implications for personal data collecting companies. [11]
Pesquisa com entrevista	Health information privacy concerns, antecedents, and information disclosure intention in online health communities. [14]
Não Informado	Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation [13]
Não Informado	Ethical issues for direct-to-consumer digital psychotherapy apps: addressing accountability, data

	protection, and consent [14]
Não Informado	Healthcare informatics and privacy [15]
Não Informado	Patienthood and participation in the digital era [16]
Não Informado	Big genetic data and its big data protection challenges [17]
Pesquisa com entrevista	The EU General Data Protection Regulation: How will it impact the regulation of research biobanks? Setting the legal frame in the Mediterranean and Eastern European area [18]
Não Informado	Moral bureaucracies and social network research [19]
Não Informado	OpenEHR and general data protection regulation: evaluation of principles and requirements [20]
Perspectiva	Does GDPR harm or benefit research participants? An EORTC point of view [21]
Não Informado	Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR [22]
Não Informado	General data protection regulation (GDPR) and pediatric medical practice in Ireland: a personal reflection [23]
Comparação	Future of data analytics in the era of the general data protection regulation in Europe [24]
Não Informado	Building trust and transparency? Challenges of the opt-out system and the secondary use of health data in England [25]
Análise sistemática	Security and Privacy in the Era of Electronic Health Records (EHRs) [26]
Não Informado	Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation [28]

O método mais utilizado para a realização dos estudos selecionados, foi o de pesquisas [5] [9][14][18], seguido pelo método de estudos de caso [1] [2]. Foi possível observar também que muitos desses estudos não citaram o método de pesquisa utilizado [6] [7][13][14][15][16][17][19][20][22] [23][25][28], sendo citados como método de pesquisa por 12 estudos.

Os métodos de pesquisa listados nos estudos selecionados são apresentados na Tabela 6.

4.9 QUAIS SÃO AS PRINCIPAIS CONCLUSÕES A QUE OS ARTIGOS OBTIVERAM?

Tabela 7. Principais conclusões reportadas pelos estudos selecionados.

Conclusões	Referência
Empresas maiores se adaptam melhor	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A Case Study [1]
leis ambíguas tornam o processo complicado	
GDPR consome tempo e é ineficiente	
organizações de saúde pública têm dificuldade em cumprir o GDPR devido a restrições financeiras	Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A Case Study in a Portuguese Healthcare Organization [2]
equipe de TI pequena	
diversos sistemas legado	
consentimento significativo ou anonimização irreversível de dados são impraticáveis ou impossíveis para pesquisas médicas intensivas em dados	Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach [3]
isenção de pesquisa	
estabelece regras mais claras para a pesquisa	The impact of the EU general data protection regulation on scientific research [4]
muito poder aos controladores e enfraquece os supervisores do estado	The risk-based approach under the new EU data protection regulation: a critical perspective [6]
considera gdpr ineficiente	
A transparência de dados é um dos métodos mais vitais para ganhar a confiança do paciente nos sistemas EHR;	A design of patients data transparency in electronic health records. [8]
EHRs ajudam a gerar bons atendimentos e melhoram a qualidade do atendimento	Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. [9]
reconhecimento público e profissional	
GDPR facilitará pesquisas consideradas de interesse público	The effect of the general data protection regulation on medical research. [10]
a empresas precisam rever estratégias, sistemas de informação e documentação	EU General Data Protection Regulation: Changes and implications for personal data collecting companies. [11]
12 aspectos a serem considerados para a implantação da GDPR	
suporte informacional e emocional aumenta	Health information privacy concerns,

intenções de divulgação de informações em OHCs	antecedents, and information disclosure intention in online health communities. [12]
benefícios e riscos são diferentes para indivíduos com status de saúde diferentes	
pseudo anonimização é considerado dado pessoal	Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation [13]
Isenção de pesquisa	
a tecnologia digital para cuidados de saúde mental pode tornar os cuidados de saúde mental menos caros	Ethical issues for direct-to-consumer digital psychotherapy apps: addressing accountability, data protection, and consent [14]
mais fáceis de acessar para muitas pessoas com problemas de saúde mental	
GDPR dificulta pesquisas genéticas	Big genetic data and its big data protection challenges [17]
Obter consentimento de todos os pacientes	
isenção de pesquisa	
tomar decisões estratégicas	Moral bureaucracies and social network research [19]
reutilizar datasets anonimizados	
subcontratação de trabalho de campo	
selecionar populações-alvo e locais convenientes	
Os princípios do openEHR estão em conformidade com o GDPR	OpenEHR and general data protection regulation: evaluation of principles and requirements [20]
saúde pública	Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR [22]
isenção de pesquisa	
interesse público	
de-identificação como método para manter a segurança e prevenir identificação por dados em processamentos de interesse público	Building trust and transparency? Challenges of the opt-out system and the secondary use of health data in England [25]
crescimento de aplicações EHR	Security and Privacy in the Era of Electronic Health Records (EHRs) [26]
EHRs ajudam a gerar bons atendimentos e melhoram a qualidade do atendimento	

As principais conclusões a que os estudos chegaram foram que a isenção de pesquisa é o melhor caminho a ser seguido por empresas da área de pesquisa em saúde [3] [13][17][22]. Ao obter a isenção essas empresas poderão coletar e processar dados sem a necessidade de consentimento do titular dos dados, mas para isso é necessário que essas empresas possam provar a relevância da pesquisa e que estão agindo de boa fé.

Já a segunda conclusão a que mais chegaram é que a pseudo anonimização é inútil para a área de pesquisa em saúde, visto que dados pseudo anonimizados são considerados dados pessoais pela GDPR [13] , pois os mesmo ainda podem ser utilizados para chegar aos dados reais dos titulares a partir de chaves que os conectam.

As principais conclusões listadas nos estudos selecionados são apresentados na Tabela 7.

4.10 QUAIS SÃO AS SUGESTÕES PARA OS TRABALHOS FUTUROS MENCIONADAS NOS ESTUDOS?

Tabela 8. Trabalhos futuros reportados pelos estudos selecionados.

Trabalhos Futuros	Referência
entrevistar mais pessoa	The GDPR and its Effects on the Management of Private Health Information at different Healthcare Providers – A Case Study [1]
entrevistar DPO	
entrevista em organizações de outros países	
mais tempo	
comparação entre os registos de auditoria disponíveis e os requisitos do GDPR e da Resolução Portuguesa do Conselho de Ministros n.º 41/2018	Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A Case Study in a Portuguese Healthcare Organization [2]
condições para isenção de pesquisa	Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach [3]
desenvolver uma implementação de prova de conceito	A design of patients data transparency in electronic health records. [8]
futuros estudos empíricos devem ser conduzidos entre empresas intensivas em dados pessoais	EU General Data Protection Regulation: Changes and implications for personal data collecting companies. [11]
investigar a implementação do GDPR em empresas de diferentes portes	
melhor apreciação da adequação da opção de pesquisa científica	Big genetic data and its big data protection challenges [17]
lista formal de requisitos da GDPR para sistemas EHR	OpenEHR and general data protection regulation: evaluation of principles and requirements [20]

Os estudos que possuem sugestões para trabalhos futuros, apresenta uma heterogeneidade de sugestões. Isso ocorre pois, por mais que o objetivo desses artigos sejam parecidos, estudar e entender os impactos das leis de proteção de dados nas empresas de saúde, os caminhos e soluções são distintos, por conta das diferenças entre as empresas e países onde esses estudos

foram realizados. Os trabalhos futuros listados nos estudos selecionados são apresentados na Tabela 8.

4.11 Discussão dos resultados

Este trabalho teve como objetivo investigar como tem ocorrido a adequação de empresas de saúde às leis de proteção de dados. Para alcançar tal meta, um estudo sistemático da literatura foi realizado. A revisão retornou 826 trabalhos dos quais 28 foram aceitos para extração. Sendo assim, este trabalho possibilitou responder às seguintes perguntas de pesquisa:

- **P1: Quais são os desafios enfrentados por empresas de saúde para adequação às leis de privacidade?** Pode-se observar que os principais desafios enfrentados dizem respeito aos princípios e direitos dos titulares apresentados pela GDPR. Foi chegado a conclusão que isso se deu por conta da adequação tardia de algumas empresas da área e também por conta do maior conhecimento dos seus direitos por parte dos titulares, que vem a negar o consentimento ao acesso e processamento de seus dados.
- **P2: Quais são as boas práticas utilizadas por empresas de saúde para adequação às leis de privacidade?** A partir do estudo realizado, foi observado que a boa prática mais utilizada pelas empresas foi o investimento de tempo e capital financeiro. Isso se dá pois quanto melhor for o entendimento a GDPR e mais for investido em pessoas e tecnologias que possam vir a auxiliar a adequação, maiores as chances de uma adequação correta.
- **P3: Qual (is) lei(s) de privacidade são mencionadas nos estudos selecionados?** A lei de privacidade mais mencionada foi a GDPR, por conta da sua abrangência internacional e também por conta da região onde os estudos foram realizados, sendo essa, em sua maioria, a Europa.
- **P4: Qual o tipo de contribuição dos estudos selecionados?** O tipo de contribuição mais observado nos estudos foi a utilização de sistemas de informação. Com isso, foi chegado a conclusão que essa preferência por sistemas de informação tornam a adequação mais fácil por esses sistemas já estarem adequados a GDPR, além de proporcionar um certo grau de proteção e privacidade aos dados.
- **P5: Qual a área de atuação dentro do contexto da saúde mencionada no estudo?** As áreas de atuação dentro do contexto de saúde que mais se destacaram foram as de atendimento de saúde e pesquisa, por conta da natureza do serviço prestado onde ocorrem uma coleta e processamento massivos de dados.
- **P6: Qual(is) impactos das leis de privacidade nas empresas de saúde?** O impacto mais observado nos estudos selecionados foi a de que os países membros da União Europeia podem fazer derrogações a GDPR. Isso se dá por conta da necessidade de coexistência entre as leis locais e a GDPR sem que se contradigam.
- **P7: Qual o método de pesquisa utilizado nos estudos selecionados?** O método de pesquisa mais utilizado pelos estudos foi de pesquisa com entrevistas de pessoas em cargos de gerência que atuam em empresas da área de saúde.

- **P8: Quais são as principais conclusões a que os artigos obtiveram?** A principal conclusão identificada foi que a isenção de pesquisa é o melhor caminho a ser seguido pelas empresas de saúde focadas em pesquisas. Isso se dá por conta da quantidade massiva de dados aos quais essas empresas precisam de consentimento para processar, algo que é extremamente trabalhoso, visto que a quantidade de titulares que precisam ser consultados também é massiva.
- **P9: Quais são as sugestões para os trabalhos futuros mencionadas nos estudos?** Foi apresentado pelos estudos uma heterogeneidade de resultados pelos estudos selecionados. Foi chegado a conclusão que isso se dá pela diferença entre os métodos de pesquisa utilizados, diferenças entre as empresas e países em que esses estudos ocorreram. Sendo assim, se houvesse uma maior homogeneidade nesses quesitos poderiam ser observadas sugestões de trabalhos futuros mais parecidas.

5 CONCLUSÃO

Todo ano milhares de pessoas procuram empresas de saúde com o intuito de tratar de algum problema de saúde e diversas pesquisas são realizadas para melhorar a qualidade de vida da sociedade. O investimento em segurança de dados e a adequação às leis de privacidade devem sempre estar em dia para garantir a segurança e privacidade dos dados pessoais dos pacientes e colaboradores. Porém com a adequação a leis de privacidades surgem desafios e dúvidas a serem sanados.

Dito isso, as principais conclusões que podem se identificar a partir da realização dessa revisão sistemática é que os estudos mais realizados ocorrem na região da Europa, visto que a grande maioria dos artigos têm como lei base de estudo a GDPR, essa que têm abrangência internacional, ou alguma outra lei local de algum país do continente.

Foi observado também uma variação na quantidade de estudos durante os anos, entre 2016 e 2021, sendo o pico em 2018. Suponhamos que isso se deu por conta de necessidade inicial de adequação e que após passado o esse período possa vir a ocorrer novamente novos picos nas futuras atualizações da GDPR.

Os estudos realizados têm se concentrado mais nas áreas de atendimento à saúde em geral e pesquisa, pois são as áreas da saúde mais afetadas pelas leis de privacidade por coletarem e processarem uma quantidade imensa de dados todos os dias por conta da própria natureza do serviço prestado.

E por fim, nas demais perguntas de pesquisa é possível notar que há heterogeneidade nos resultados, onde é difícil chegar a um consenso entre os artigos, por conta das diferenças entre as empresas e países onde foram realizados os estudos.

5.1 TRABALHOS FUTUROS

Seria interessante para trabalhos futuros como é o comportamento da realização de estudos sobre o tema após edições realizadas as leis de privacidade, a fim de identificar a repetição do padrão observado pela revisão sistemática realizada, em relação a quantidade de publicações de estudos por ano.

É interessante também a realização do mesmo estudo em empresas da área de saúde em relação à LGPD, lei de privacidade brasileira que tem como base a GDPR. E também poder fazer a comparação entre o estado da arte e o estado da prática.

REFERÊNCIAS

[1] PRZYROWSKI, Catrin. **The GDPR and its effects on the management of private health information at different healthcare providers: A case study**. 2018. Trabalho de Conclusão de Curso. University of Twente.

[2] SANTOS-PEREIRA, Cátia et al. Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A Case Study in a Portuguese Healthcare Organization. In: **HEALTHINF**. 2020. p. 555-562.

[3] MOSTERT, Menno et al. Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. **European Journal of Human Genetics**, v. 24, n. 7, p. 956-960, 2016.

[4] CHASSANG, Gauthier. The impact of the EU general data protection regulation on scientific research. **ecancermedicalscience**, v. 11, 2017.

[5] HATHALIYA, Jigna J.; TANWAR, Sudeep. An exhaustive survey on security and privacy issues in Healthcare 4.0. **Computer Communications**, v. 153, p. 311-335, 2020.

[6] GONÇALVES, Maria Eduarda. The risk-based approach under the new EU data protection regulation: a critical perspective. **Journal of Risk Research**, v. 23, n. 2, p. 139-152, 2020.

[7] DELOITTE. 2018 global health care outlook: the evolution of smart health care. 2018.

[8] JAYABALAN, Manoj; THIRUCHELVAM, Vinesh. A design of patients data transparency in electronic health records. In: **2017 IEEE International Symposium on Consumer Electronics (ISCE)**. IEEE, 2017. p. 9-10.

[9] ENTZERIDOU, Eleni; MARKOPOULOU, Evgenia; MOLLAKI, Vasiliki. Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. **International journal of medical informatics**, v. 110, p. 98-107, 2018.

[10] RUMBOLD, John Mark Michael; PIERSCIONEK, Barbara. The effect of the general data protection regulation on medical research. **Journal of medical Internet research**, v. 19, n. 2, p. e7108, 2017.

[11] TIKKINEN-PIRI, Christina; ROHUNEN, Anna; MARKKULA, Jouni. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. **Computer Law & Security Review**, v. 34, n. 1, p. 134-153, 2018.

[12] ZHANG, Xing et al. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. **Information & Management**, v. 55, n. 4, p. 482-493, 2018.

[13] SHABANI, Mahsa; BORRY, Pascal. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. **European Journal of Human Genetics**, v. 26, n. 2, p. 149-156, 2018.

[14] MARTINEZ-MARTIN, Nicole et al. Ethical issues for direct-to-consumer digital psychotherapy apps: addressing accountability, data protection, and consent. **JMIR mental health**, v. 5, n. 2, p. e9423, 2018.

[15] IYENGAR, Arun; KUNDU, Ashish; PALLIS, George. Healthcare informatics and privacy. **IEEE Internet Computing**, v. 22, n. 2, p. 29-31, 2018.

[16] ERIKAINEN, Sonja et al. Patienthood and participation in the digital era. **Digital Health**, v. 5, p. 2055207619845546, 2019.

[17] QUINN, Paul; QUINN, Liam. Big genetic data and its big data protection challenges. **Computer law & security review**, v. 34, n. 5, p. 1000-1018, 2018.

[18] PENASA, Simone et al. The EU General Data Protection Regulation: How will it impact the regulation of research biobanks? Setting the legal frame in the Mediterranean and Eastern European area. **Medical Law International**, v. 18, n. 4, p. 241-255, 2018.

[19] MOLINA, José Luis; BORGATTI, Stephen P. Moral bureaucracies and social network research. **Social Networks**, v. 67, p. 13-19, 2021.

[20] GONÇALVES-FERREIRA, Duarte et al. OpenEHR and general data protection regulation: evaluation of principles and requirements. **JMIR medical informatics**, v. 7, n. 1, p. e9845, 2019.

[21] NEGROUK, Anastassia; LACOMBE, Denis. Does GDPR harm or benefit research participants? An EORTC point of view. **The Lancet Oncology**, v. 19, n. 10, p. 1278-1280, 2018.

[22] MÉSZÁROS, János; HO, Chih-hsing. Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR. **Hungarian Journal of Legal Studies**, v. 59, n. 4, p. 403-419, 2018.

[23] PHILIP, Roy K. General data protection regulation (GDPR) and paediatric medical practice in Ireland: a personal reflection. **Irish Journal of Medical Science (1971-)**, v. 188, n. 2, p. 721-724, 2019.

[24] KOLASA, Katarzyna et al. Future of data analytics in the era of the general data protection regulation in Europe. **PharmacoEconomics**, v. 38, n. 10, p. 1021-1029, 2020.

[25] MESZAROS, Janos; HO, Chih-hsing. Building trust and transparency? Challenges of the opt-out system and the secondary use of health data in England. **Medical Law International**, v. 19, n. 2-3, p. 159-181, 2019.

[26] CHAWKI, Mohamed. Security and Privacy in the Era of Electronic Health Records (EHRs). **RAIS Journal for Social Sciences**, v. 5, n. 1, p. 1-12, 2021.

[27] SHABANI, Mahsa; BORRY, Pascal. Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. **European Journal of Human Genetics**, v. 26, n. 2, p. 149-156, 2018.

[28] MINSSEN, Timo; RAJAM, Neethu; BOGERS, Marcel. Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation. **Science and Public Policy**, v. 47, n. 5, p. 616-626, 2020.

[29] Terra, Augusto, Jéssyka Vilela, Mariana Peixoto. A catalog of quality criteria to guide the assessment of applications' privacy policies. **Workshop on Requirements Engineering (WER)**, 2022.

[30] Wohlin, Claes. "Guidelines for snowballing in systematic literature studies and a replication in software engineering." **In *Proceedings of the 18th international conference on evaluation and assessment in software engineering***, pp. 1-10. 2014.

[31] Rees, Dorian. Cyber attack in healthcare: the position across Europe. **Pinsent Mansons.** 18 de Junho de 2021. Out-Law. Disponível em: <https://www.pinsentmasons.com/out-law/analysis/cyber-attacks-healthcare-europe>.

[32] Estados Unidos. *US Department of Health & Human Services*. *Office for Civil Rights (OCR)*. Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People. Washington, DC. 2021.

[33] União Europeia. Parlamento Europeu. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>.

[34] TENE, Omer. Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. **Ohio St. LJ**, v. 74, p. 1217, 2013.