UNIVERSIDADE FEDERAL DE SÃO CARLOS (UFSCar)
CENTRO DE EDUCAÇÃO E CIÊNCIAS HUMANAS (CECH)
CURSO DE BIBLIOTECONOMIA E CIÊNCIA DA INFORMAÇÃO

RANIEL ALESSANDRO ANDRADE SANTOS

ASPECTOS DA BIBLIOTECONOMIA E CIÊNCIA DA INFORMAÇÃO PARA A PRIVACIDADE DE DADOS E AMBIENTES DIGITAIS

SÃO CARLOS/SP
2022

RANIEL ALESSANDRO ANDRADE SANTOS

ASPECTOS DA BIBLIOTECONOMIA E CIÊNCIA DA INFORMAÇÃO PARA A PRIVACIDADE DE DADOS E AMBIENTES DIGITAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Biblioteconomia e Ciência da Informação como requisito para obtenção do título de Bacharel em Biblioteconomia e Ciência da Informação pela Universidade Federal de São Carlos (UFSCar).

Orientadora: Prof.ª Dr.ª Ana Carolina Simionato Arakaki

SÃO CARLOS/SP
2022

Santos, Raniel Alessandro Andrade

Aspectos da Biblioteconomia e Ciência da Informação para a privacidade de dados e ambientes digitais / Raniel Alessandro Andrade Santos -- 2022.
49f.

TCC (Graduação) - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Ana Carolina Simionato Arakaki
Banca Examinadora: Ariadne Chloë Mary Furnival, Januário Albino Nhacuongue
Bibliografia

1. Ciência da informação. 2. Privacidade de dados. 3. Ambientes digitais. I. Santos, Raniel Alessandro Andrade. II. Título.

RANIEL ALESSANDRO ANDRADE SANTOS

ASPECTOS DA BIBLIOTECONOMIA E CIÊNCIA DA INFORMAÇÃO PARA A PRIVACIDADE DE DADOS E AMBIENTES DIGITAIS

Trabalho de Conclusão de Curso apresentado ao Curso de Biblioteconomia e Ciência da Informação como requisito para obtenção do título de Bacharel em Biblioteconomia e Ciência da Informação pela Universidade Federal de São Carlos (UFSCar).

Aprovado em: ____/____/____

BANCA EXAMINADORA

_____

Profa. Dra. Ana Carolina Simionato Arakaki
Universidade Federal de São Carlos (UFSCar)

_____

Profa. Dra. Ariadne Chloë Mary Furnival
Universidade Federal de São Carlos (UFSCar)

_____

Prof. Dr. Januário Albino Nhacuongue
Universidade Federal de São Carlos (UFSCar)

AGRADECIMENTOS

Aos meus pais,
por todo o amparo e apoio que fez com que eu pudesse chegar até aqui

À Brenda, Jéssica, Rhuan, Babi, José, Tiago, Ton, Ingrid, Laura, Larissa, Felipes e todas as pessoas incríveis que tive a oportunidade de conhecer Brasil a fora, obrigado por cada risada, cada viagem, cada festa, cada copo de cerveja e cada momento que fez com que esses anos de graduação pudessem ser tão incríveis

À todos os profissionais do DCI, que me ajudaram nessa trajetória, cada um me ensinou algo à sua maneira e tudo isso contribuiu para a percepção que tenho hoje da Biblioteconomia e Ciência da Informação. Agradeço em especial a Profa. Ana Carolina, por ter me orientado e ser uma docente e pessoa tão incrível

Ao PET BCI e às tutoras Luciana e Paula,
por todo o aprendizado e crescimento que tive na minha passagem pelo grupo

À UFSCar,
por ter aberto aberto suas portas e me acolhido, hoje saio uma pessoa muito melhor

À todos que de alguma forma fizeram parte dessa história
Muito obrigado!

RESUMO

A falsa sensação de segurança que os usuários têm em relação aos seus dados pessoais, faz com que eles se tornem cada vez mais vulneráveis a diversos tipos de fraude, desde vazamentos até sua comercialização. Aliado a isso, surgem questões em torno da privacidade, como um conceito que amplia seu significado dentro e fora da tecnologia conforme o tempo passa. Pensando nisso, leis foram criadas para a proteção dos dados, de forma a garantir a privacidade dos usuários. Assim, o presente trabalho dedica-se à temática da privacidade de dados, com foco em ambientes e jogos digitais, analisando o papel das leis de proteção de dados na segurança dos dados pessoais do indivíduo, frente à empresas e organizações. Será investigado o âmbito acadêmico nacional da temática. Deste ponto, incita-se como problemática de pesquisa: os dados cedidos para as empresas enquanto seus serviços são utilizados permanecem, de fato, privados? Tendo como foco tal problemática, o objetivo é identificar o funcionamento da privacidade de dados, vista da perspectiva da Biblioteconomia e Ciência da Informação. Diante do propósito investigativo, trata-se de uma pesquisa de natureza teórica, classificada como investigação qualitativa e, quanto aos procedimentos, trata-se de uma pesquisa bibliográfica. Em primeiro momento, fez-se uma investigação teórica para fundamentação acerca das legislações vigentes, privacidade e segurança dos dados. Ao fim, verificou-se que a partir de uma análise bibliométrica que as pesquisas acerca da privacidade de dados tem aumentado ao longo dos anos, contudo ainda é necessário mais trabalhos ao redor de privacidade de ambientes e jogos digitais.

Palavras-chave: Proteção de Dados Pessoais**.** Privacidade. Proteção de Dados. Dados Pessoais. Lei Geral de Proteção de Dados Pessoais. Lei de Acesso à Informação.

ABSTRACT

The false sense of security that the users have regarding their personal data makes them even more vulnerable to several types of fraud, from leaks to its commercialization. In addition, questions regarding privacy arise as a broad concept inside and outside technology as time goes by. With that in mind, laws have been created for data protection, in order to ensure user's privacy. Thus, this study is dedicated to discuss data privacy, focusing on digital games and environments and analyzing the role played by data protection laws in the security of each individual's personal data towards companies and organizations. Here, the national academic scope of this subject will be explored. From this perspective, the following research problem is incited: Does the data provided to companies while their services are being used remain, in fact, private? Focusing on this research problem, the aim of this study is to identify how data privacy work, from the Librarianship and Information Science perspective. For the investigative purpose, this study is a theoretical research classified as qualitative investigation and, regarding its procedures, it is a bibliographical research. Initially, theoretical research was carried out to substantiate the aspects of the current legislation, data privacy and security. As a result, the bibliometric analysis revealed that research about data privacy has increased over the years, however, more studies are needed regarding the data privacy of digital games and environments.

Keywords**:** Personal Data Protection**.** Privacy. Data Protection. Personal Data. General Personal Data Protection Law. Information Access Law.

LISTA DE GRÁFICOS

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AGNU	Assembleia Geral das Nações Unidas
ALPDP	Anteprojeto de Lei de Proteção de Dados Pessoais
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
APPI	*Act on the Protection of Personal Information*
BCI	Biblioteconomia e Ciência da Informação
CA	Califórnia
CC	Código Civil
CCPA	*California Consumer Privacy Act*
CDC	Código de Defesa do Consumidor
CI	Ciência da Informação
CF	Constituição Federal
CF/88	Constituição Federal de 1988
CGI.br	Comitê Gestor da Internet Brasileira
CRFB/88	Constituição Federal da República Federativa do Brasil de 1988
DA	Dados Abertos
DDE	*Data Driven Economy*
DPO	*Data Protection Officer*
DUDH	Declaração Universal dos Direitos Humanos
DSAR	*Data Subject Access Request*
EEE	Espaço Econômico Europeu
EUA	Estados Unidos da América
FGV	Fundação Getulio Vargas
GDA	Guia de Dados Abertos
GDPR	*General Data Protection Regulation*
IPv6	*Internet Protocol*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LMCI	Lei Marco Civil da Internet
MCI	Marco Civil da Internet
MJ	Ministério da Justiça

ONU	Organização das Nações Unidas
PIDCP	Pacto Internacional sobre os Direitos Civis e Políticos
PIPEDA	*Personal Information Protection and Electronic Documents Act*
RFB	República Federativa do Brasil
RGPD	Regulamento Geral sobre a Proteção de Dados
TCC	Trabalho de Conclusão de Curso
TICs	Tecnologias da Informação e Comunicação
UE	União Europeia
UFSCar	Universidade Federal de São Carlos

SUMÁRIO

INTRODUÇÃO

Privacidade é um conceito que ao longo dos anos amplia seu significado conforme a tecnologia avança. Segundo o dicionário Houaiss, a privacidade significa “[...] vida privada, particular, íntima [...]”. A vida privada vem se modificando com o passar dos tempos, uma vez que a internet possibilita transmitir a vida cotidiana e as opiniões de modo ágil e confortável. A falsa sensação de segurança que as companhias passam, muitas vezes se trata de uma estratégia para adquirir os dados dos usuários visando a sua comercialização.

Os dados são a menor unidade de informação gerados no ambiente informacional. O uso dos dados comercializados costuma ir para empresas especializadas em *marketing*, onde fazem o tratamento dos dados com o intuito de gerar lucros para o mercado, adaptando os produtos para os gostos dos usuários e para a produção de anúncios direcionados de modo a impactar os usuários tidos como possíveis clientes.

Verificando a situação dos usuários, leis foram criadas pensando na proteção dos dados, leis essas que garantem a privacidade dos usuários. A Constituição Federal da República Federativa do Brasil, de 1988, assegura o direito à privacidade, assim como o Marco Civil da Internet, de 2014 e a Lei Geral de Proteção de Dados Pessoais - LGPD, de 2018, que visa trazer uma série de exigências acerca da coleta, armazenamento e tratamento de dados pessoais dos usuários.

É importante ressaltar que, além das leis nacionais, a privacidade também é garantida e está sob tutela de órgãos internacionais como a Organização das Nações Unidas – ONU e a Declaração Universal dos Direitos Humanos - DUDH.

A privacidade em ambientes digitais se configura em medidas legais que servem para a proteção tanto da empresa como para o usuário e com o intuito de que o usuário possa usufruir das redes de forma segura. Tais medidas podem se resumir em dois contratos eletrônicos: “Termos de Uso” e "Política de Privacidade”.

Os Termos de Uso estabelecem as regras para utilização do aplicativo ou site, apresentando os deveres e os direitos dos usuários como também da plataforma. A Política de Privacidade define as informações específicas que serão coletadas pela

plataforma e que serão registradas e armazenadas no ambiente e utilizadas para o tratamento dos dados.

A Política de Privacidade é um modelo desenvolvido de acordo com as necessidades dos aplicativos/sites e dos usuários e por conta disso, cada política é distinta e possui objetivos que se diferenciam mesmo que levemente. A privacidade em jogos digitais envolve fatores importantes como a faixa etária do usuário, por conter menores de idade, localização e ambientes seguros que o jogo possa rodar.

A Política de Privacidade permite também coletar informações, cujos dados são transferidos para empresas que fazem o tratamento necessário e criam propagandas ideais para cada tipo de usuário. Na indústria de jogos a propaganda é direcionada para pessoas com perfis de jogadores, ou seja, usuários que pesquisam na internet sobre jogos, que baixam os jogos no celular ou no computador e que mantêm cadastro em sites de estúdios de jogos.

O jogo *Pokémon Go*, lançado em julho de 2016 é um exemplo dessa análise. Trata-se de um aplicativo *mobile* que utiliza dados de localização do usuário em tempo real para renderizar todo o game, como observado pela Figura 1.

Figura 1 – Interface do Pokemón GO

Fonte: Avila, Gallego e Noyes (2020).

Um dos tópicos de discussão levantados diante do aplicativo é que o jogo digital continua obtendo dados mesmo ao ser fechado pelo usuário, gerando desconfianças levantadas em fóruns online, usuários ou quem se interessa pelo jogo.

Diante disso, se faz necessária uma análise das legislações vigentes e as que entraram em vigor para que se possa entender o cenário atual e as perspectivas que cerceiam o direito à privacidade e seus desdobramentos.

1.1 Definição do problema

Por essa perspectiva, incita-se como problemática de pesquisa: como bibliotecários, profissionais da informação, tratam em suas pesquisas os dados pessoais cedidos para as empresas de jogos digitais enquanto seus serviços?

Assim, para sustentação do problema objetiva-se verificar a importância das legislações vigentes para proteção e privacidade dos dados, salientando a importância do comprometimento de empresas de jogos digitais e o papel do governo.

1.2 Objetivos

A partir do exposto, o presente trabalho tem como objetivo geral identificar a temática de privacidade de dados e jogos digitais, em pesquisas nacionais da área de Biblioteconomia e Ciência da Informação.

Os objetivos específicos são:

- Contextualizar a temática de privacidade de dados;
- Analisar o papel das leis de proteção de dados na segurança dos dados pessoais do indivíduo;
- Compreendendo sobre a importância da segurança dos dados, sugerindo melhorias que beneficiem e alertem usuários e empresas de jogos digitais;
- Identificar a temática de privacidade em jogos digitais em âmbito científico nacional, descrevendo as publicações indexadas pela BRAPCI.

1.3 Justificativa

A temática da proposta justifica-se pelo interesse na área ter se sobressaído se comparado a outras disciplinas realizadas na Universidade Federal de São Carlos (UFSCar) na área de Biblioteconomia e Ciência da Informação, junto ao fato de que jogos digitais sempre foram, em âmbito pessoal, atrativos e presentes.

Desse ponto, surge a necessidade de saber se os dados cedidos para as empresas enquanto seus serviços são utilizados permanecem, de fato, privados.

A Constituição Federal traz, em seu artigo 5º, inciso X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”.

Enquanto o Código Civil (CC) diz que: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

Contudo, o cenário atual é preocupante já que, para ter acesso à maioria dos aplicativos, incluindo relacionados a jogos digitais, é necessário aceitar os termos de uso e ceder dados para as empresas, que por sua vez, devem seguir as legislações e manter tais dados privados.

Esse cenário traz as novas leis criadas para garantir a proteção dos dados, são elas o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018), que serão analisadas no decorrer deste trabalho.

Essas indagações motivaram o início deste trabalho e espera-se que os resultados satisfaçam as necessidades dos possíveis leitores e pesquisadores, inspirando trabalhos na área de Ciência da Informação e nas demais áreas do conhecimento.

1.4 Procedimentos metodológicos

Diante do propósito investigativo, a pesquisa apresentada pode ser classificada como pesquisa de investigação qualitativa e quantitativa. Quanto à sua natureza, pode ser classificada como uma pesquisa teórica, visto construção da teoria com base na pesquisa bibliográfica, acerca do tema abordado.

Em relação aos procedimentos, trata-se de uma pesquisa bibliográfica com uma análise bibliométrica, devido à reunião de informações que auxiliarão no desenvolvimento do projeto.

Partindo dessa premissa, o plano de trabalho para a execução do seguinte Trabalho de Conclusão de Curso foi baseado em seis etapas, conforme a seguir:

1ª etapa: Levantamento bibliográfico e seleção do material obtido – Busca de materiais bibliográficos, acerca da temática proposta frente a embasamento teórico a fim de fundamentar a pesquisa com base na literatura. Sendo assim, o levantamento bibliográfico será realizado em nível nacional e internacional, considerando a política de diferentes regiões.

2ª etapa: Leitura, interpretação, análise e sistematização das informações – Leitura do material bibliográfico selecionado e utilizado para o desenvolvimento da fundamentação teórica.

3ª etapa: Análise e estabelecimento das características fundamentais extraídas da literatura – Para estabelecimento de análise e reflexão de características principais encontradas na bibliografia referente ao tema, consolidando assim, a análise do objeto de estudo.

- Para a contextualização teórica foram utilizadas fontes bibliográficas como fundamentação teórica com base em pesquisas realizadas pelos autores: Bernardo, Santos, Santos Junior e Bento (2021); Dias e Oliveira (2019); Jorge, Oliveira, Machado, Lima e Otre (2020); Lima e Monteiro (2013); Marchiori e Lopes (2016); Oliveira e Araújo (2020); Santos e Sant'Ana (2013); Setzer (2001); Shintaku, Sousa, Costa, Moura e Macedo (2021); Silveira e Avelino (2016); Sousa, Barrancos e Maia (2019).
- Nesse sentido, propõe-se em um primeiro momento uma investigação teórica a respeito das temáticas que englobam a privacidade de dados. Em segundo momento, pretende-se analisar a jurisdição brasileira e internacional que envolve o tema.
- Em terceiro momento, após análise e reflexão, planeja-se verificar os riscos e maneiras de prevenção, a fim de orientar os usuários, já que esse também é um papel do bibliotecário.

4ª etapa: Sistematização do estudo qualitativo e quantitativo de cunho teórico – Abrangendo o objetivo geral da pesquisa em questão, por meio de análise e reflexão referente ao tema abordado.

Esta pesquisa caracteriza-se como quantitativa com a natureza descritiva de análise dos dados, a partir de uma abordagem bibliométrica, com a finalidade de analisar e reunir indicadores bibliométricos da produção científica sobre privacidade no contexto nacional. A bibliometria consiste em uma "[...] técnica quantitativa e estatística de medição dos índices de produção e disseminação do conhecimento científico" (ARAÚJO, 2006, p.12).

A coleta de dados foi realizada na base de dados BRAPCI, abrangendo todo o período de publicação da base. O estudo foi dividido em três etapas que serão descritas a seguir:

- Etapa 1) Coleta dos dados: a coleta de dados foi realizada na base BRAPCI. Estratégia de busca: "Privacidade"; "Privacidade de dados". Os termos foram buscados de forma individual, e posteriormente foi feita a ligação entre os termos de forma manual. O levantamento foi realizado no dia 23 de setembro de 2022. Ao todo foram recuperados 119 trabalhos. Foram analisadas as seguintes informações: autor, título e ano.
- Etapa 2) Padronização dos dados: formatação, padronizando os nomes dos autores e título dos periódicos.
- Etapa 3) Análise dos dados: elaboração de gráficos e análise dos dados coletados, buscando extrair informações para este estudo.

5ª etapa: Elaboração e redação final da pesquisa – Desenvolvimento do Trabalho de Conclusão de Curso (TCC) para a defesa. Essa etapa não se constitui unicamente do momento final da pesquisa, como também, de um processo construtivo e contínuo conjunto da orientadora e aluno.

6ª etapa: Divulgação da pesquisa – Apresentação do Trabalho de Conclusão de Curso (TCC) finalizado visando divulgação à comunidade científica dos resultados obtidos com o desenvolvimento do estudo.

1.5 Estrutura do trabalho

O presente Trabalho de Conclusão de Curso (TCC) está estruturado do seguinte modo:

Capítulo 1 – Contextualizar o tema e a pesquisa, apresentando a introdução, a definição do problema, os objetivos o geral e os específicos, justificativa, procedimentos metodológicos e estrutura do trabalho.

Capítulo 2 – Apresenta a Fundamentação Teórica, abrangendo os subcapítulos de Privacidade dos Dados; LGPD; Legislações: papel das leis de proteção de dados na segurança dos dados pessoais do indivíduo; Empresas produtoras de jogos: a segurança dos dados nas empresas e; a Importância da Segurança dos Dados.

Capítulo 3 – Apresenta a sugestão de melhorias que beneficiem e alertem os usuários e empresas, convergindo com o objetivo específico proposto.

Capítulo 4 – Apresenta as considerações finais sobre a pesquisa realizada.

Referências – São apresentadas as referências consultadas que formam o corpus teórico do trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Dados pessoais e segurança digital

Dados e informação são assuntos recorrentes e bastante discutidos na Biblioteconomia e Ciência da Informação. Desde a criação da Imprensa de Gutenberg no século XV, houve uma produção massiva de documentos que perdurou por séculos. Até que no século XX com o surgimento e avanço de novas tecnologias, os dados, informações e documentos passam a ser armazenados em ambiente virtual, e ganham um valor ainda maior do que tinham, paralelo a isso, o direito à privacidade é cada vez mais debatido, porém sem muitos avanços na prática.

Para entender melhor essa dinâmica, parte-se do princípio de definir alguns conceitos básicos. Entende-se os dados como o estado mais bruto que antecede a informação e o conhecimento. Para Setzer (2001) os dados podem ser definidos como uma sequência de símbolos quantificados ou quantificáveis, visto de uma forma puramente sintática. O autor tem a visão de dados como elementos matemáticos, que são armazenados, processados e virtualmente ligados a outros dados através de um computador (SETZER, 2001).

Santos e Sant'Ana (2013, p. 205) definem dados como:

> [...] uma unidade de conteúdo necessariamente relacionada a determinado contexto e composta pela tríade entidade, atributo e valor, de tal forma que, mesmo que não esteja explícito o detalhamento sobre contexto do conteúdo, ele deverá estar disponível de modo implícito no utilizador, permitindo, portanto, sua plena interpretação. (SANTOS; SANT'ANA, 2013, p. 205).

Considera-se assim, como a mínima expressão de qualquer tipo de conteúdo, podendo ser representado em diversos tipos de recursos. E com a popularização de tantos tipos de dispositivos, somando à difusão da internet no mundo, criou-se uma situação em que as Tecnologias da Informação (TI) adentram e se tornaram imprescindíveis em nossas vidas.

> O crescente uso das tecnologias da informação e da comunicação, em especial da Internet, imprimiu maior dinamicidade às relações econômicas, à participação política e às interações sociais, redesenhando as formas de ser e estar no mundo. Em nenhum outro momento histórico foi tão fácil e rápido acessar informações, produzir e compartilhar conteúdos, comunicar e interagir em sites de redes sociais, blogs e microblogs, tudo de maneira instantânea. O intenso desenvolvimento capitaneado pelo segmento de Tecnologias da Informação (TI) acelera ainda mais esse processo, pois a cada dia são lançados no mercado novos equipamentos, aplicativos,

> plataformas e ferramentas que maximizam a experiência de navegação na web, o que faz com que um número crescente de pessoas almeje a inclusão digital (SILVA;SILVA, 2013, p. 2).

Ao mesmo tempo, deve-se ter um olhar crítico e notar que dados e informações no geral se tornaram cada vez mais difíceis de serem controladas, sujeitas a ataques e cada vez menos privadas, como também trazem Silva e Silva (2013, p. 2)

> Mas ao lado desse panorama de otimismo e de novas oportunidades também se revelam inéditos problemas e desafios decorrentes do grande fluxo informacional, especialmente quando as informações assumem a forma de dados pessoais e saem do controle do seu titular. Essa situação de vulnerabilidade tanto pode ocorrer quando os dados são espontaneamente disponibilizados nas interações sociais, como ocorre com publicações feitas em sites de redes sociais; nos casos em que são recolhidos pelo fornecedor para permitir a abertura de contas que garantirão o acesso a serviços e produtos ou nas situações de captura indevida por meio de algum programa espião. A pluralidade de formas de recolhimento de informações demonstra a complexidade do tema, pois mesmo o internauta mais cauteloso e com seletivas atuações no ambiente virtual não fica a salvo de sofrer ataques aos seus dados pessoais (SILVA; SILVA, 2013, p. 2).

A partir disso torna-se fundamental entender um pouco mais a respeito do nosso direito à privacidade e como essa era digital o tornou cada vez mais importante e menos garantido.

2.2 A constituição de privacidade

Segundo os autores, Warren e Brandeis (1890), a privacidade pode ser definida como *“the right to be let alone”*, traduzindo literalmente significa “O direito de ser deixado em paz”. O artigo *The Right To Privacy* foi publicado em 1890 e é uma obra relevante até hoje. Nele, os autores consideram a violação desses direitos como uma ofensa que afeta a individualidade, dignidade, independência e honra do indivíduo.

Décadas depois, o termo privacidade ainda é o objeto de estudo para diversos estudos. Martins e Bastos (1989) apontam que a privacidade pode ser definida como a:

> [...] faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre essa área da manifestação existencial do ser humano. (BASTOS; MARTINS, 1989, p. 63).

Os autores também detalham que o conceito sobre privacidade evolui junto à sociedade, sendo um tema visto com bastante importância. Contudo, no século XX com o surgimento da internet, o assunto passou a ser visto da forma como hoje é

conhecido, ou seja, a privacidade em outras esferas da intimidade, tanto da vida privada como do ambiente virtual.

Para além da internet e de sistemas inteligentes de coleta de dados, um ponto importante a ser destacado são as redes sociais e plataformas que detém dados dos usuários para que eles possam acessar seus serviços ou produtos. E quase sempre a justificativa é a de oferecer mais qualidade ao usuário.

> Coletamos informações para fornecer serviços melhores a todos os nossos usuários, desde descobrir coisas básicas, como o idioma que eles falam, até coisas mais complexas, como anúncios que o usuário pode considerar mais úteis, as pessoas on-line que são mais importantes para o usuário ou os vídeos do YouTube dos quais o usuário poderá gostar (GOOGLE, 201-).

A privacidade se trata de um direito fundamental, reservado a todo cidadão e o direito à privacidade se encontra preservado sob a tutela de algumas entidades, como no caso da Organização das Nações Unidas (ONU) que promulgou o artigo 12° da Declaração Universal dos Direitos Humanos, de 1948, que diz,

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Ao contrário de intromissões ou ataques toda pessoa tem direito à proteção da lei (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948, não paginado)

No Brasil, a proteção de dados pessoais também é debatida e pesquisada, tanto no meio acadêmico, quanto no Congresso. Segundo Dias e Oliveira (2019),

> O direito à privacidade tem um grau de suma importância na Constituição Brasileira. Considerado como um dos direitos de personalidade e, portanto, é revestido de característica própria de direito fundamental e cláusula pétrea. Em decorrência da fragilidade do objeto (privacidade), pode ser violado mais facilmente. (DIAS; OLIVEIRA, 2019, p. 72)

Além da Constituição Federal, tem-se alguns outros instrumentos que visam manter os dados pessoais preservados, como a Lei de Proteção de Dados Pessoais, Marco Civil da Internet, entre outras. Em seu art. 5º, inciso X, a Constituição declara que “[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988).

Essa preocupação com a vida privada surgiu na constituinte após o Brasil passar por um regime ditatorial que durou de 1964 a 1988. Nesse período ditatorial, o governo agiu com autoritarismo e utilizava a inteligência do Estado para conseguir as

mais diversas informações privadas de pessoas que eles consideravam inimigas. No entanto, Venturini (2016) afirma que esses abusos continuaram e continuam acontecendo até hoje, mesmo após a conquista da democracia, necessita-se de leis que protejam o cidadão e que essas leis sejam acatadas.

Tem se tornado cada vez mais comum escândalos de espionagem e vazamentos de dados que envolvem tanto agências governamentais quanto empresas privadas. O Brasil chegou a ser, inclusive, condenado na Corte Internacional por realizar interceptações consideradas ilegais.

> [...] não se trata apenas de proteger cidadãos das intrusões do Estado na vida privada, mas de garantir que o tratamento de dados por parte do setor privado obedeça a princípios básicos que incluem adequação, necessidade, transparência, segurança, não discriminação, entre outros. O respeito a tais princípios e ao direito à privacidade busca preservar a autonomia e a liberdade e se torna ainda mais central para o funcionamento da democracia e o respeito aos direitos fundamentais. (VENTURINI, 2016)

Partindo desse ponto, é necessário observar a importância em se tomar iniciativas que garantam a segurança de dados e informações.

A segurança da informação se trata de medidas voltadas para defesa dos dados, mantendo o sigilo, valor e integridade dos dados. Para Dhillon (2004) a definição sobre segurança dos dados, ainda abarca confidencialidade, integridade, responsabilidade, honestidade, confiança e a ética de todos os agentes envolvidos. No momento em que um usuário aceita os termos de uso de determinado jogo, serviço, *software* ou aplicativos, ele precisa ter a certeza de que seus dados serão resguardados de quaisquer ações desonestas, seja de origem interna ou externa à empresa.

As falhas na segurança ou ataques que levam a vazamentos ou corrompimentos de dados podem acontecer em diferentes níveis desde a fonte até o destino. Autores como Stallings (1999) e Pereira (2005) trazem essa problemática desde a década de 90 e mais de 20 anos depois, ainda se vê com bastante recorrência casos de atos ilegais envolvendo dados e informações privadas.

Jorge et al. (2020) destaca que a revolução informacional foi apoiada pela nova era das Tecnologias da Informação e Comunicação (TICs). Ao citar a sociedade da informação, destaca que cada organização nesse novo molde de sociedade, passou a ser uma organização de informação, sendo cada organismo de informação e, ao final, isso tornou a informação o recurso primordial na organização do que a sociedade desenvolve e constrói.

Ao trazer Mattelart (2002 apud JORGE et al., 2020) os autores destacam que os avanços tecnológicos na propagação da informação aceleraram a desigualdade social, partindo da construção de monopólios informacionais que são utilizados como instrumentos para detentores das novas tecnologias tomarem o poder e se tornarem dominantes em diversos aspectos da sociedade, como aspectos econômicos, sociais e políticos.

Nesse aspecto, surge a sociedade digital que está passando por um processo de assimilação, segundo Mattelart (2002 apud JORGE et al., 2020), o que gera novas maneiras de interações sociais e modifica, por sua vez, modos anteriores de vida social.

Partindo dos termos trazidos por Drucker (1969, 2000 apud JORGE et al., 2020), os termos “economia do conhecimento” e “sociedade do conhecimento”, enfatizam o conhecimento como um forte recurso social e econômico da sociedade, colocando a informação como o recurso central da sociedade da informação.

Assim, a internet passa a ser o centro desse processo ao prover dados de diferentes naturezas. A sociedade, dessa forma, passa a ser caracterizada por comportamentos encontrados em sites, mídias online, sites governamentais, blogs e fóruns, redes sociais e, indiretamente, por meio do processamento informatizado, dados são capturados para monitorar as atividades realizadas no mundo real e virtual.

Nesse contexto de dados capturados e monitoramento de atividades realizadas no mundo real e virtual, surgem questões de privacidade nos ambientes digitais que se configuram em medidas legais, servindo para a proteção tanto da organização como para o indivíduo.

As legislações sobre proteção de dados incluem: o tratamento dos dados pessoais em meios digitais, tanto por pessoa natural/física, quanto por pessoa jurídica (de direito público ou privado); possui como objetivo principal proteger os direitos de liberdade e privacidade, além do desenvolvimento livre de personalidade da pessoa natural.

No aspecto de privacidade, em seu projeto, Shintaku et al. (2021) diz que, diante das exigências legislativas, surge a necessidade de criar um modelo de adaptação do sistema de informação governamental que seja direcionado ao uso de identificação, como, login e cadastro de usuários através do uso de mídias sociais de maior alcance, como o Facebook e o Google.

Com isso, Shintaku et al. (2021) destaca que é importante considerar as políticas de privacidade que devem estar de acordo com as normas que as orientam, partindo de boas práticas de gestão, planejamento e implementação de Sistemas da Informação. Nesse caso, sistemas de informação governamental que, além de tratar de aspectos de desenvolvimento do próprio sistema, considera-se também a segurança para proteção da privacidade.

No Brasil, as empresas ainda estão se adaptando à LGPD, porém, na Europa e demais países, a segurança dos dados já é tida como prática habitual. Além disso, a população está começando a compreender o que significa a segurança dos dados e o papel de quem contribui para que essa segurança seja efetiva.

O portal Consumidor Moderno (2021) relata que o país está no meio de um processo de entendimento e que há uma evolução em andamento. Traz ainda um questionamento quanto ao cenário em que o Brasil se encontra em meio a proteção e segurança de dados pessoais:

> O Brasil é um dos países com o maior número de vítimas de ataques cibernéticos no mundo e, recentemente, sofreu um dos maiores vazamentos de dados da sua história que pode ter exposto 223 milhões de brasileiros. A questão está na ordem do dia, o que leva ao questionamento: como estão a leis de proteção de dados em outros países e onde o Brasil se encontra nesse cenário? (CONSUMIDOR MODERNO, 2021).

Para Milagre (2021 *apud* CONSUMIDOR MODERNO, 2021), antes da LGPD entrar em vigor, ocorriam diversos vazamentos de dados que eram ocultados pelas empresas e demais pessoas jurídicas. Hoje, caso algum vazamento ocorra, as empresas devem comunicar aos titulares e à Autoridade Nacional de Proteção de Dados, além de procurar medidas que reduzam esse risco.

Lima e Monteiro (2013) destacam que o Brasil, ao contrário de outros países que compartilham do mesmo cenário mundial de dados, ainda não possui uma proteção adequada para dados de natureza pessoal. Mesmo que já sejam consideradas proteções à privacidade dos indivíduos, estabelecidas pela Constituição Federal de 1988, como também pelo Código Civil, pela Lei de Acesso à Informação (LAI) e pelo Código de Defesa do Consumidor (CDC), os autores salientam que o país está ainda distante do nível de adequação e garantia legislativa aos dados, como as da Europa, Canadá, Estados Unidos, entre outros.

Por essa razão, carecendo de uma legislação nacional com o objetivo de estipular um marco regulatório adequado, os autores idealizaram o Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP), proveniente do trabalho da Fundação Getúlio Vargas (FGV) e do Ministério da Justiça.

Lima e Monteiro (2013) fundamentaram para seu projeto diversas leis já em vigência no âmbito internacional, como, por exemplo, a Diretiva Europeia de Proteção de Dados Pessoais e a Lei de Proteção de Dados Canadense que foram analisadas em seu trabalho que está nas referências do presente trabalho de conclusão de curso.

Como menciona o portal Consumidor Moderno (2021) com sede em São Paulo, a partir do momento que a Lei Geral de Proteção de Dados entrou em vigor, no Brasil, no ano de 2020, o país começou a ser visto como quem se preocupa com a segurança de dados e informações de sua população, sendo uma garantia sobre como os dados dos brasileiros são coletados, armazenados e utilizados, ainda que esteja em fase de adoção pelas empresas e instituições. É por esse motivo que a LGPD traz maior segurança à população local, por meio de seus regulamentos de proteção de dados.

Segundo o portal Consumidor Moderno (2021), os países membros da União Europeia garantem a segurança dos cidadãos europeus há décadas, através da *General Data Protection Regulation* (GDPR).

A GDPR, em português, é chamada de RGPD, ou seja, é o Regulamento Geral sobre a Proteção de Dados, considerada a regulamentação mais completa sobre o tema de segurança de dados no mundo, servindo até mesmo como inspiração para o escrito da LGPD, como explica-se, a seguir:

> A legislação europeia, em português chamada de Regulamento Geral sobre a Proteção de Dados, ou RGPD, válida em todos os países da União Europeia e do Espaço Econômico Europeu (EEE), é considerada a mais completa regulamentação sobre segurança de dados no mundo e inspirou o próprio texto da LGPD. (CONSUMIDOR MODERNO, 2021).

Como salienta o portal Consumidor Moderno (2021), quando a RGPD entrou em vigor na Europa, ela serviu de impulso para que os demais países buscassem uma legislação nessa nova era e, ao movimentar a economia da Europa, gerou novos empregos na área de segurança dos dados.

No Brasil, além da movimentação da economia, pode ocorrer parecido com o que foi na Europa, a partir do momento que as empresas forem adaptando-se à lei de proteção de dados e, com isso, haverá a necessidade de contratar profissionais ou

empresas especializadas para controle e tratamento de seus dados. (CONSUMIDOR MODERNO, 2021).

A partir de então, o Portal Consumidor Moderno (2021) perpassa pelas demais leis, que serão apresentadas a seguir. Outra legislação de proteção de dados presente no mundo é a regulamentação na Califórnia (CA), estado no oeste dos EUA. Sabe-se que, ainda não existe uma regulamentação para todo o país americano, porém, na CA, desde o ano de 2020, existe em vigor uma espécie de método de defesa do consumidor com influências da RGPD da Europa, isto é, o *California Consumer Privacy Act of 2018*, ou, CCPA.

O *California Consumer Privacy Act* (CCPA), ou, também denominada como Lei de Privacidade do Consumidor da Califórnia, é uma legislação do estado que objetiva aperfeiçoar os direitos de privacidade e proteção do consumidor para a população da Califórnia.

A lei da CCPA surgiu na necessidade de a Califórnia proteger melhor a segurança de dados de sua população, uma vez que não existe uma única lei geral de proteção de dados no país. Ela reúne regras a serem seguidas pelas empresas que lidam com os dados pessoais, na Califórnia - EUA e, surge também a partir da regulamentação europeia, GDPR. (GATEFY, 2021).

Segundo o Gatefy (2021) a lei foi aprovada no ano de 2018 e entrou em vigor no início de 2020. Seu ponto principal concede aos residentes da Califórnia mais direitos sobre seus dados, desde acessá-los, saber como eles são usados e, até mesmo, proibir o uso de seus dados pessoais.

Por outro lado, desde o ano de 2000, no Canadá, existe em vigor, uma legislação nacional chamada *Personal Information Protection and Electronic Documents Act*, a PIPEDA, ou, traduzindo, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos.

Para compreender a PIPEDA, precisa-se primeiro falar sobre a *Privacy Act*, tida como a primeira legislação no Canadá sobre privacidade de dados e regulamento do uso de dados pessoais pelo Governo. (DALMASSO, 2020).

Segundo Dalmasso (2020), a *Privacy Act* é também chamada de *Loi sur la protection des renseignements personnels*. A lei entrou em vigência no ano de 1983. Alguns anos depois, viria a PIPEDA, com vigência em 2000.

A *Privacy Act*, por exemplo, traz o direito de o cidadão não apenas acessar, como corrigir informações pessoais que o Governo do Canadá detém sobre seus

dados, esse acesso. Segundo Dalmasso (2020), pode ser feito por meio de conferência do documento ou por meio de uma cópia do documento ofertada pela autoridade.

Já a PIPEDA, segundo o autor, tem como objetivo regulamentar o uso e divulgação de informações pessoais de um indivíduo, de maneira pela qual se reconheça o direito à privacidade de cada indivíduo em relação às suas informações pessoais e, para isso, deve-se reconhecer também qual a finalidade de uma ou mais ou organização ao coletar, utilizar ou divulgar informações pessoais, lembrando que a organização precisa de um propósito minimamente razoável.

Logo, é possível perceber que, enquanto a *Privacy Act* trata sobre como o governo federal lida com informações pessoais, a PIPEDA retrata como as empresas lidam com informações pessoais. (DALMASSO, 2020). Por fim, no Japão, como menciona o portal Consumidor Moderno (2021)

> [...] a privacidade de dados era regida pela Lei de Proteção de Informações Pessoais, de 2003. Em 2017, através da emenda APPI, a legislação se tornou mais ampla a ponto de a União Europeia considerar o país oriental totalmente adequado quanto à proteção de dados. (CONSUMIDOR MODERNO, 2021).

A *Act on the Protection of Personal Information* (APPI), ou, Lei de Proteção de Informações Pessoais, é a principal legislação sobre dados pessoais no Japão que se aplica tanto a pessoas físicas, quanto a pessoas jurídicas que processam informações pessoais. No entanto, a APPI distingue informação pessoal de dados pessoais, sendo as informações pessoais as que fazem parte de um banco de dados de informações pessoais. (AWS, 2022).

Outros dois países, segundo o portal Consumidor Moderno (2020) com legislações no ramo de segurança de dados pessoais bem estabelecidas são: a Argentina e a Nova Zelândia.

No primeiro, há em vigor a Lei de Proteção de Dados Pessoais que foi aprovada no ano 2000 e objetiva limitar o uso dos dados apenas para a atividade que consentida pelo cidadão. Enquanto, no segundo, a Lei de Privacidade de 1993 serve como base para regular a segurança de dados, embora ainda exista uma atualização dessa lei em andamento.

Sousa, Barrancos e Maia (2019) destacam que nos últimos anos, o grande volume de dados e informações produzidos em alta escala, devido às tecnologias da

informação e comunicação, geraram a necessidade de controle dos dados para que a garantia de direitos fundamentais previstos na constituição acerca do tratamento de dados pessoais seja realizada, como destacam a seguir:

> A importância do acesso à informação e os reflexos na sociedade, advindos com a grande quantidade de conteúdo que se encontra disponível, por meio das tecnologias da informação e comunicação, conduz ao reconhecimento da disponibilidade das mesmas como fonte ampla de disseminação de informação. (SOUSA; BARRANCOS; MAIA, 2019, p. 239).

Dessa maneira, Sousa, Barrancos e Maia (2019) analisaram o tratamento de dados pessoais em relação ao poder público junto aos reflexos provenientes da Lei de Acesso à Informação (LAI), avaliando aspectos de proteção da privacidade, além de considerar o consentimento um requisito essencial, especifica os direitos do titular previstos na Lei Geral de Proteção de Dados.

Segundo as autoras, a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados vieram do objetivo de proteger os direitos fundamentais de liberdade e de privacidade, de forma a garantir a transparência sobre o tratamento, a circulação, as informações e a acessibilidade dos dados pessoais.

As autoras examinam o tratamento de dados pessoais pelo poder público ao considerar, por exemplo, a LAI e sua ligação com os prazos e procedimentos e prazos sobre a garantia da proteção de dados e informações pessoais.

Além disso, as autoras destacam o porquê é necessário que haja diálogo das fontes jurídicas, para que se tenha uma circulação e um tratamento dos dados e informações pessoais, dessa maneira, seria possível visar “[...] o exercício da democracia e promoção da dignidade da pessoa humana.” (SOUSA; BARRANCOS; MAIA, 2019).

A necessidade de acesso à informação passou a ser reconhecida internacionalmente em aspectos de direitos econômicos, sociais e culturais. O Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), de 1966 aprovado pela Assembleia Geral das Nações Unidas (AGNU) diz, em seu artigo 19 e item 2, que todos possuem como direito, buscar, receber e transmitir informações e ideias de todas as maneiras, sejam elas, escrita, impressa, oral, pela arte ou qualquer outro meio. (SOUSA; BARRANCOS; MAIA, 2019).

Sousa, Barrancos e Maia (2018), assim, afirmam a necessidade de ampliação em relação à proteção de barreiras na aplicação da LAI, em relação à proteção de

dados pessoais para o tratamento de informações, também pessoais, mas com transparência e preservação da intimidade, privacidade, liberdade e garantias individuais que são previstas pela constituição referente aos órgãos públicos.

O tratamento de dados aborda todas as atividades praticadas com os dados pessoais dos indivíduos, com início pela coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão e, por fim, na extração. (SOUSA; BARRANCOS; MAIA, 2019).

Dessa forma, como salientam as autoras, objetiva-se o estabelecimento de regras sobre como as instituições privadas e públicas devem tratar dos dados pessoais e a importância do cuidado no tratamento para o controle nessa circulação de dados e informações pessoais de cada pessoa.

A privacidade, como mencionam, Sousa, Barrancos e Maia (2019) é tratada na Constituição Federal de 1988, no artigo 5º, inciso X, ao considerar invioláveis a vida privada e intimidade, assim como, considera também no artigo 5º e inciso XII, a interceptação das comunicações telefônicas, telegráfica ou, do aspecto tratado de dados.

Os direitos de acesso e complementação de informações também são destacados no artigo 5º, mas, dessa vez no inciso XIV, determinando que a todos é assegurado o acesso à informação e, inciso XXXIII, em que todos possuem o direito de receber dos órgãos públicos, as informações de seu interesse particular, interesse coletivo ou geral, quando o sigilo for imprescindível à segurança da sociedade e do Estado. (SOUSA; BARRANCOS; MAIA, 2019).

Nesse contexto, segundo as autoras, a Lei Geral de Proteção de Dados nasce para favorecer o controle dos indivíduos sobre seus dados pessoais, em respeito à privacidade; liberdade de expressão, de informação, de comunicação e de opinião, entre outros. Enquanto, a proteção de dados, vem para proporcionar a devida segurança para que informações pessoais circulem de maneira adequada.

Assim sendo, o controle por meio do consentimento do titular, favorece o que antes era: privacidade constituída pelo cidadão, junto à informação e segredo, para uma mudança significativa que passa a ser: cidadão, informação e controle. (SOUSA; BARRANCOS; MAIA, 2019).

Como enfatizam as autoras, é dessa forma que a proteção da privacidade é relacionada ao controle dos dados pessoais, sobre o dever, por parte das empresas que tratam dos dados pessoais, em informar com transparência o que fazem com esses dados, como direito do titular, garantindo também, a "[...] autodeterminação informativa, como forma do titular decidir o que, quando e como devem ser utilizados os seus dados." (SOUSA; BARRANCOS; MAIA, 2019).

A respeito dos direitos do titular na proteção de dados pessoais, o objetivo é garantir que o titular tenha a liberdade de assegurar que seus dados são tratados de forma segura e transparente, de forma a cumprir seu objetivo.

Como enfatizam as autoras, a LGPD examina o tratamento dos dados pessoais de cada indivíduo pelo poder público considerando a LAI em relação aos procedimentos e prazos estipulados, de maneira a garantir ao titular a proteção de seus dados e suas informações pessoais.

Sobre o citado direito do titular, cabe mencionar o DSAR. No *Data Subject Access Request* (DSAR) ou Requisição de Acesso aos Dados do Titular, tanto na LGPD, quanto na GDPR, os cidadãos possuem direitos que devem ser cumpridos pelas organizações que controlam os dados pessoais de cada indivíduo, ou seja, o DSAR é uma das formas de o cidadão solicitar por um ou mais desses direitos. (AIQON, 2020).

Por exemplo, o direito de acesso aos seus próprios dados, permitindo com que o indivíduo saiba quais dados pessoais a organização coletou dele. Assim, o titular se mantém ciente sobre quais dados foram coletados e pode assim, verificar a legalidade do tratamento desses dados. (AIQON, 2020).

Os aspectos que envolvem a proteção da privacidade, ao considerarem o consentimento como requisito principal, busca mudanças em relação à cultura do sigilo no controle de dados e informações pessoais dos cidadãos, pautados pela Lei Geral de Proteção de Dados. (SOUSA; BARRANCOS; MAIA, 2019).

Assim, como salientam as autoras, as legislações expõem quais são os direitos do titular, como o acesso aos seus dados, a correção de dados incompletos ou desatualizados, a portabilidade dos dados e eliminação dos dados pessoais tratados com o consentimento do titular.

O consentimento então, ao ser colocado como ponto importante, serve de ponto de partida para que a lei seja também colocada em prática, a partir da participação dos cidadãos titulares.

Ainda, sobre as requisições de acesso aos dados do titular ou DSAR, a partir do momento em que as organizações são requisitadas a trazer medidas de proteção e segurança aos dados pessoais, impedindo qualquer vazamento de dados, algumas requisições de acesso aos dados do titular devem cumprir com alguns passos, como, por exemplo, designar uma pessoa responsável em sua organização para intermediar o titular.

Essa pessoa será o denominado *Data Protection Officer* (DPO) que deve ser o intermédio entre os titulares de dados, sendo o supervisor das estratégias de proteção de dados para a LGPD, assim como, outros requisitos envolvem desenvolver diretrizes de manuseamento de dados, identificar a base legal para o processamento de dados pessoais, entre outros. (AIQON, 2020).

A política de privacidade ligada à proteção de dados demonstra transparência e credibilidade, à qual os indivíduos ao tomarem conhecimento de que seus dados serão utilizados, podem autorizar ou não o seu uso e coleta. Sendo essa, uma das medidas mais importantes ao impedir o uso indevido de dados, invasão de privacidade, entre outros problemas.

Bernardo et al. (2021), sobre a invasão de privacidade, diz que a transformação tecnológica na sociedade trouxe múltiplos benefícios, como a facilidade em fazer compras, pedir delivery, além de benefícios no processo de ensino e aprendizagem em configuração atual. Porém, também múltiplos resultados negativos como a disseminação de informação de fontes não confiáveis, facilidade da invasão de dados e privacidade, dados violados e insegurança no acesso às redes.

> Ter seus dados violados não é uma situação que parece ser algo que pode ser resolvido de forma tranquila, por se tratar de uma problemática que requer atenção e cuidado é importante que os usuários possam ampliar seus conhecimentos em relação à lei que regulamenta os usuários que não estão totalmente seguros, os recursos midiáticos tem cada vez mais apresentado casos de invasão de dados de figuras marcantes na sociedade que vai desde artistas até personalidades do governo, o que causa uma série de problemas que afetam a vida pessoal e social do indivíduo. (BERNARDO et al., 2021, p. 14).

Por isso, é de suma importância que as organizações informem ao indivíduo o destino dos dados fornecidos, uma vez que eles podem ser compartilhados e, até mesmo, vendidos, como os cookies, ou serem apagados do banco de dados depois de um determinado período. É uma forma de garantir que as pessoas não terão suas

vidas e dados expostos por terceiros sem seu consentimento. (BERNARDO et al., 2021).

Marchiori e Lopes (2016) discutem sobre os termos de uso e políticas de privacidade de sites, retratam que normalmente, esses sites apresentam “[...] corresponsabilidades de uso/navegação e, idealmente, deveriam esclarecer, respaldar e sustentar vínculos de transparência entre as organizações e seus clientes/usuários, em especial quanto à amplitude da proteção de dados pessoais.”

Assim, abordam os princípios de informação equitativa que visam sustentar uma política de privacidade voltada ao compromisso ético em troca de informações, como mostra a seguir,

> Os princípios de informação equitativa – principalmente em ambientes de presença e serviços online – se traduzem em diretrizes que sustentam uma política de privacidade voltada ao compromisso ético na troca de informações, e que vem em auxílio à percepção de uma relação respeitosa entre empresa e cliente, pautada por vínculos de transparência. (MARCHIORI; LOPES, 2016).

Ainda no aspecto de privacidade na internet, Lima e Monteiro (2013) destacam que a Agência Nacional de Telecomunicações (ANATEL) e o Comitê Gestor da Internet Brasileira (CGI.br), dispõe do princípio da neutralidade como um dos fundamentos pelo qual o provedor deve manter sigilo em relação aos dados de seus clientes ou usuários, sem transferir a terceiros, até mesmo quando cometerem atos supostamente ilícitos, “[...] não podendo revelá-los senão mediante ordem judicial.”

Oliveira e Araújo (2020), destacam que quando a Administração Pública age no campo da privacidade e de proteção aos dados pessoais, o tratamento também é um ato administrativo e, por isso, “[...] detém como pressuposto de validade a finalidade pública, que neste caso, está intrinsecamente relacionada ao interesse público que alicerça a operação de uso desses dados”.

Os autores destacam que a própria LGPD declara, em seu artigo 7º e inciso III, o tratamento e compartilhamento de dados pessoais pela Administração Pública quando forem precisos para a execução das políticas públicas previstas em leis e regulamentos, como também, estabelecidas em contratos, convênios, entre outros.

Para os autores, o uso compartilhado de dados pessoais pelo poder público deve atender a finalidades específicas e adequadas de execução das políticas públicas, como atribuição legal por órgãos e entidades públicas, de forma a respeitar

princípios de proteção de dados pessoais da lei em questão. (OLIVEIRA; ARAÚJO, 2020).

A LGPD considera como dado pessoal, toda informação relacionada a pessoa “natural identificada ou identificável”, considerando dados de nome completo, dados de endereço, dados de localização, assim como, identificadores online, de renda, etc. O dado pessoal sensível, por sua vez, se trata de dados sobre origem racial ou étnica do indivíduo, sua religião, sua opinião política ou filiação a sindicato, dados sobre sua saúde, vida sexual, dados genéticos, dados biométricos vinculados a pessoa natural/física. Por isso, os dados pessoais sensíveis, conforme transcrito acima, são dados que podem causar discriminação ao seu titular, sobretudo por guardarem informações pessoais sensíveis do indivíduo, aumentando ainda mais a responsabilidade das organizações que gerenciam esses dados. (OLIVEIRA; ARAÚJO, 2020).

Essa é a responsabilidade do poder público no tratamento de dados pessoais e dados pessoais sensíveis. Logo, segundo Oliveira e Araújo (2020), existem maneiras de proteger os dados pessoais e os dados sensíveis, por meio de técnicas de anonimização, criptografia e *tokenização*, por exemplo.

Esses três procedimentos surgem como alternativas às possíveis ameaças e garantia de segurança. A anonimização é citada diretamente na LGPD e se trata de uma técnica utilizada no tratamento e impossibilita a associação entre o dado e o indivíduo. Criptografia pode ser definida como a transformação de um determinado dado de um formato legível, para um formato codificado. Já a *tokenização* é um tipo de tecnologia cujo processo substitui dados por códigos indecifráveis, preservando sua estrutura, é o mesmo princípio que norteia o blockchain.

Por fim, Oliveira e Araújo (2020), também enfatizam que a publicação de dados públicos em formato aberto está prevista na LAI e, segundo o Guia de Dados Abertos (GDA), a partir do momento em que todos os dados públicos devem ser abertos, deve-se analisar que nem todos os dados são, de fato, públicos. Por isso, segundo os autores, sob responsabilidade do governo está avaliar essas possibilidades de abertura de dados, de forma transparente.

2.3 Lei Geral de Proteção de Dados (LGPD)

Na era digital se tornou cada vez mais comuns acordos entre governos e empresas de tecnologias, acordos esses que utilizam os dados da população quase sempre sem o seu conhecimento. A Lei Geral de Proteção de Dados (LGPD) é muito recente e suas sanções sequer estão em vigor.

Para proteger o cidadão não basta apenas o Estado não espionar seu povo, mas deve também garantir que essas informações privadas não sejam obtidas de forma irregular por empresas que passaram a comercializar dados pessoais.

> O mercado de dados pessoais é cada vez mais relevante na sociedade informacional e pode ser entendido como as interações econômicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente. (SILVEIRA; AVELINO; SOUZA, 2016)

Com o tempo, os dados deixaram de ser apenas informações que dizem respeito à vida privada de uma pessoa e passaram a servir os interesses do recente mercado, sem que o cidadão comum se desse conta. Entendendo essa nova abordagem para o uso de dados pessoais, Rodotà (2008) traz que,

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso de dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em “controle” (RODOTÀ, 2008, p. 37)

Muitas vezes, por não ter a noção que os dados são coletados ou utilizados, os usuários ficam fragilizados e vulneráveis àqueles que mantêm seus dados sob controle.

Como dito anteriormente, o Brasil possui leis a favor da segurança de privacidade do usuário, entre elas, a LGPD, que vem entrando em vigor de maneira escalonada e sendo totalmente disposta em agosto de 2021. No seu art. 1° diz:

> Esta Lei 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. (BRASIL, 2018)

A Lei Geral de Proteção de Dados (LGPD) é fiscalizada pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD), órgão federal responsável por proteger os dados pessoais e por implementar e fiscalizar se a LGPD está sendo adotada.

O Marco Civil da Internet é também conhecido como Lei 12.965, de 2014, que visa “[...] estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil". No art 3°, inciso II e III garantem a proteção da privacidade e a proteção dos dados pessoais. Compreende-se que se trata de uma espécie de regulamentador de atividades no meio eletrônico, que antes eram tratadas por legislações não específicas, no entanto, não foi capaz de sanar algumas lacunas, como Bastos (2018) destaca

> Necessitava-se, portanto, de maior regulamentação no âmbito do direito digital. Assim, o Marco Civil da Internet se destacou por prever princípios, garantias, direitos e deveres para o uso da Internet no Brasil. No entanto, ele próprio deixava uma importante lacuna: a questão dos dados pessoais no direito digital. Reconheceu as relações jurídico-virtuais e os efeitos delas no ordenamento. Dispôs, por exemplo, acerca dos crimes cibernéticos. Mas deixou de abordar como os dados fornecidos pelos usuários poderiam ser utilizados pelas empresas (BASTOS, 2018, p. 1).

A comercialização de dados é comum e bastante rentável, cuja comercialização pode ser denominada como mercado de dados. Os dados são adquiridos pelo Estado e pelas empresas de diversas maneiras, podendo ser por usos de formulários para clientes ou de outras formas onde o usuário tem uma participação ativa, porém o uso mais comum é a utilização de *cookies*.

Os *cookies* permitem que os conteúdos pesquisados e clicados sejam salvos, sendo que muitas vezes o envio desses *cookies* não é informado para os usuários, tornando-os assim, alvos fáceis para o marketing.

O *marketing* é o uso estratégico do mercado para adaptar os produtos, os tornando objetos de desejo para o consumidor. Os dados pessoais auxiliam o marketing a identificar os gostos de cada usuário. Os dados pessoais não contêm apenas o nome, endereço e o IP, ele armazena também os sites mais acessados, listas de compras ou qualquer informação relevante para os interesses econômicos.

Segundo Silveira, Avelino e Souza (2016), a coleta do mercado de dados pode ser dividida em quatro camadas, sendo elas: coleta e armazenamento de dados; processamento e mineração de dados; análise e formação de amostras e a camada de modulação.

Na primeira camada a coleta de dados ocorre através de sites, formulários, ferramentas de pesquisas e rastreamento de navegação; na segunda camada os dados são tratados e organizados com o objetivo de fazer com que os perfis pessoais sejam mais detalhados; na terceira camada, análise e formação de amostras, é que envolve a equipe de marketing, onde desenvolve estratégias de anúncios direcionados, que são propagandas personalizadas e focadas em apenas uma pessoa; e na quarta camada, a de modulação que identifica as ofertas de produtos e serviços, as vendas de produtos que foram alcançadas através de anúncios direcionados.

A política de privacidade é um contrato eletrônico que garante o uso dos dados dos usuários e a forma que os dados dos aplicativos e sites podem ser utilizados, além de isentar o servidor de quaisquer responsabilidades resultantes da falta de consentimento. Cada ambiente digital tem sua necessidade específica para a criação de uma política de privacidade e de termos de usos.

A política de privacidade tem como principal função estabelecer quais informações serão obtidas e como serão utilizadas pelo site e como acontecerá a transferência desses dados a terceiros, como para o marketing, por exemplo.

Os termos de uso são as regras de como se deve utilizar o site e os aplicativos, também é local que se encontrará a descrição de serviço prestado e define como o usuário deverá usar a plataforma, logo, é um documento formado por cláusulas que protegem legalmente o site.

3 RESULTADOS

3.1 A segurança dos dados nas empresas

Quem já não ouviu falar nas maiores empresas produtoras de games ou jogos eletrônicos do mundo? Desde a Nintendo até a Microsoft, Sony, Tencent, Roblox Corporation, Apple, entre outras.

Machado, Santuchi e Carletti (2018) destacam em seus estudos, que empresas que atuam em algum setor da cadeia de jogos têm crescido cada vez mais. Esses, por sua vez, influenciam a sociedade de forma geral, em um mundo onde cada vez mais as pessoas estão conectadas através dos jogos.

Em 2011, uma invasão à rede de jogos online da Sony serviu de exemplo para que as demais empresas do setor de games pensassem em melhorias para seus sistemas de segurança de dados e, por isso, a partir de então, a segurança de dados se tornou fonte de preocupação em games online.

> O episódio da invasão à rede de jogos online da Sony, a Playstation Network, ocorrido em 2011, é certamente o maior caso de roubo de dados de usuários de games online. O serviço ficou inativo por mais de 20 dias e estimativas apontaram que 77 milhões de usuários em vários países possam ter sido afetados. (FECOMERCIO-SP, 2015).

Tecnologia, dados e segurança são uma relação primordial para a segurança dos usuários de jogos online, assim como, gamificação e segurança da informação. Um dos principais crimes cibernéticos ocorre pela falha dos usuários, pelo acesso de links desconhecidos ou maliciosos nas redes, que instalam, por sua vez, programas de espionagem ou de vírus nos equipamentos pessoais, até mesmo nos da empresa. (LUDOS PRO, [s.d.]).

Por outro lado, existem os decorrentes vazamentos de dados por essas empresas que estão, ao mesmo tempo, propensas a sofrerem invasões de rede.

Segundo o site Ilumeo ([s.d.]), o uso de dados nas principais desenvolvedoras de jogos faz parte do uso do Data Science para alavancar seus negócios. Nesse aspecto, a maioria das empresas coletam dados de usuários, sendo eles: tempo, histórico no jogo, pontos de desistência, pontuações, comportamentos, interações, entre outros dados. Esses insights são depois utilizados de diversas maneiras em áreas do marketing, para experiência do cliente, vendas, etc.

Ainda assim, as desenvolvedoras têm se preocupado e direcionando ações para detecção de qualquer mínima atividade maliciosa, de forma a melhorar a experiência e segurança do usuário em seus jogos. (ILUMEO, [s.d.]).

Mas, e a proteção de dados de usuários de games? Uma vez que a LGPD exige que os dados pessoais dos usuários podem apenas ser tratados mediante consentimento do mesmo, o titular (pessoa física), o documento jurídico mais indicado, enquanto o assunto ainda se desenvolve cada vez mais, é o uso dos Termos de Uso e da Política de Privacidade, de forma a deixar esclarecido ao usuário a dinâmica do jogo digital, formas de pagamento, obrigações de usuário versus empresa e, aviso prévio de quais dados dos usuários serão coletados e tratados, como bem salienta o site da equipe Parceiro Legal (2019).

A versão mais recente do Protocolo de Internet, chamada de IPv6, preocupou-se com outra forma de assegurar a integridade, autenticidade e confidencialidade dos dados dos usuários, como explicado a seguir:

> [...] a versão mais recente do *Internet Protocol* (IPv6), se preocupou em garantir, por meio do IPSec (IP Security), a criptografia de pacotes, assegurando integridade, autenticidade e confidencialidade. Todavia, isso não pode significar descuido com a segurança dos dados que trafegam e que serão coletados, devendo ser utilizados mecanismos tecnológicos e jurídicos para uma verdadeira proteção. (PARCEIRO LEGAL, 2019).

Com isso, segundo o site da equipe Parceiro Legal (2019), essa nova economia guiada por dados, ou também, *Data Driven Economy* (DDE), proporcionará melhor qualidade de vida, pois, uma vez que, o fluxo de informações passará por um crescimento exponencial, como é o caso do IPv6, a velocidade na troca de informações e criação de algoritmos serão maiores e mais precisos, assumindo papel de diagnósticos e classificações dos usuários. Porém, é importante ressaltar que nem sempre esses diagnósticos dos usuários são corretos em sua totalidade.

Por isso, a coleta de dados e seu uso pelos desenvolvedores de jogos, tem trazido discussões interessantes sobre o tema, a partir do momento em que é realizada a coleta de dados pessoais, tanto do dispositivo utilizado, quanto do jogador. Assim, essa nova economia ser ágil é de extrema importância, ao buscar também melhorias e soluções inovadoras. Porém, é sempre importante ressaltar que o manuseio de dados coletados e seu uso, independente da finalidade, deve ser sempre rodeado de cuidados e atenção. (PARCEIRO LEGAL, 2019).

Para os autores Knapp, Morris, Marshall, Byrd (2009) o primeiro e mais importante passo para a organização se preparar contra eventuais ataques ou falhas em relação aos dados, é desenvolver seu conjunto de políticas de segurança da informação.

Um ponto importante a se destacar quando se fala sobre segurança de dados e a implementação da LGPD, é que essas iniciativas beneficiam tanto o usuário final, que terá seus dados e direitos resguardados, quanto a empresa, que se adequa à legislação e se protege de quaisquer riscos. Tendo isso em mente, Casarotto (2021) no blog rockcontent, traz uma série de iniciativas que empresas de qualquer segmento, em especial as que trabalham com o mundo digital, devem seguir:

- Mapear os dados: Identificar todos os dados que a empresa coleta é fundamental para o controle e tratamento, além de prevenir quaisquer riscos judiciais que as empresas venham a incorrer.
- Reformular documentos: Após mapear todo tipo de contrato e documento relacionado ao tratamento de dados, explicitando sua finalidade de forma clara e transparente, principalmente no que diz respeito ao acesso por parte de terceiros.
- Definição de políticas internas: Empresas de todos os portes devem ter políticas internas bem definidas, além de um programa de governança em privacidade, no qual a proteção deve ser prevista antes mesmo de um projeto ser idealizado.
- Adoção de medidas de segurança da informação: A adoção de ferramentas de segurança da informação e protocolos evitam incidentes e exposições de dados indevidos. Alguns podem ser facilmente implementados como criptografias de dados e termos de responsabilidade e confidencialidade entre funcionários da corporação.
- Conscientização da equipe: É necessário que todos os colaboradores que lidam direta ou indiretamente ou dados de clientes, estejam cientes dos seus deveres e obrigações no que tange às novas legislações, logo, promover treinamentos e capacitação a respeito da LGPD e a importância da segurança de dados de forma geral.
- Definir encarregados: Se existe um papel a ser desempenhado pela empresa no que diz respeito à LGPD, o ideal é que se tenha um ou mais profissionais

capacitados para serem encarregados de organizar as políticas e procedimentos.

- Definir equipe de implementação: As pessoas envolvidas nessa etapa, além de qualificadas, devem ter a noção de todo o fluxo de dados para que seja possível mapear, revisar e monitorar toda a estratégia que será adotada da implementação em diante.

No mais, cada um desses pontos deve ser visto com cuidado e principalmente observados a partir do modelo de negócios de cada empresa, já que cada uma vai ter suas particularidades de acordo com o tipo de dados pessoais que ela armazena.

3.2 Mapeamento bibliométrico

Para fins de estudo, foi feito um mapeamento bibliométrico na base da Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (BRAPCI) com o intuito de analisar todas as publicações que citam o termo “privacidade” e, partir disso, segmentar até a temática de jogos digitais.

A princípio foram identificados 119 artigos, que, após o afundamento dos dados, trazem informações bastante relevantes.

Os tópicos discutidos nesta análise serão: ano de publicação e os principais autores que publicam a respeito do tema proposto.

No gráfico 5, nota-se que a maior parte dos artigos que envolvem a privacidade de dados foram publicados nos anos de 2020, 2016 respectivamente, essas datas são de um período muito próximo em que o Marco Civil da Internet e a LGPD entraram em vigor.

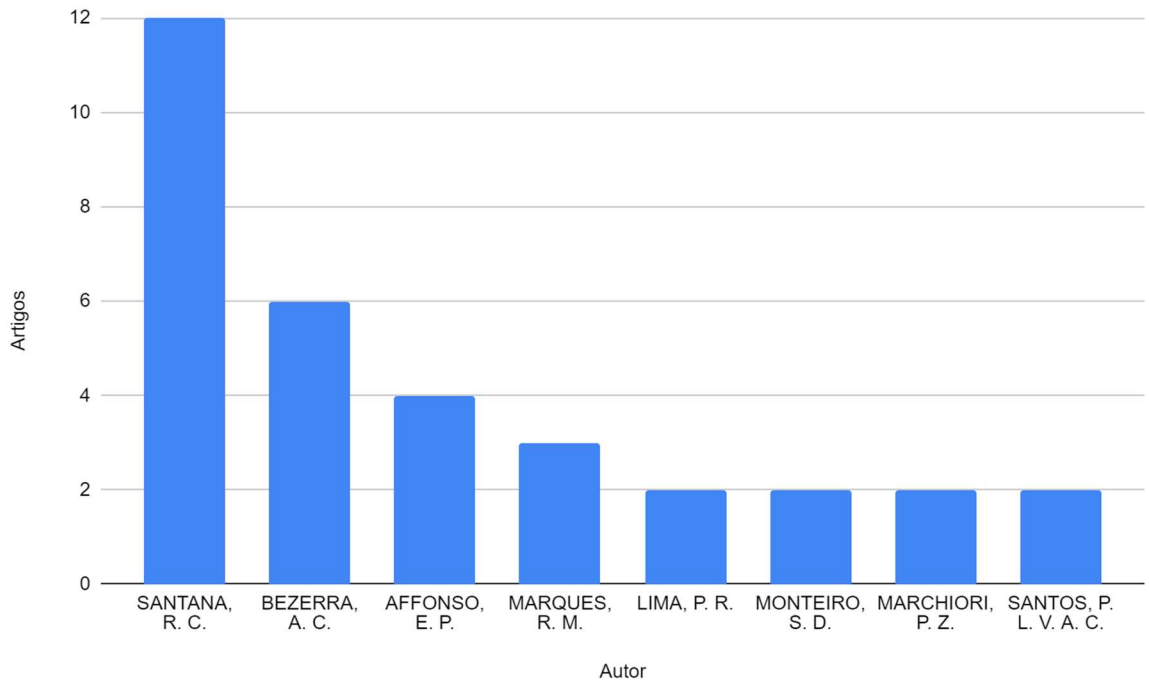
Gráfico 1 - Relação entre publicações por ano

Fonte: Elaboração própria

Após a leitura e análise dos artigos de acordo com as principais palavras-chave que englobam este trabalho, observa-se que o tema foi discutido em frequência constante desde 2009 em maior número no ano de 2020. Após o ano de 2020, a publicação decaiu. Nesta observação pondera-se a relação com a Pandemia de Coronavírus a partir de 2019, que afetou grande parte das publicações e da organização dos periódicos.

No intuito de identificar as diferentes autorias dos pesquisadores que mais desenvolveram pesquisas sobre a temática, observa-se o gráfico 6.

Gráfico 2 - Autores e quantidade de publicações



Fonte: Elaboração própria

Pode-se observar que SANTANA, R. C. é quem mais publica artigos relacionados, seguido de BEZERRA, A. C. e AFFONSO, E. P. Os trabalhos de SANTANA, R. C. são bastante interessantes e amplos, abordando desde a privacidade de dados no gerenciamento de repositórios até artigos que abordam a teoria econômica na Ciência da Informação.

BEZERRA, A. C. também publica artigos bastante variados, falando desde teoria matemática à ética, vigilância e cultura algorítmica. Os demais temas abordados pelos autores envolvem questões sobre a pandemia de Coronavírus, arquivos digitais, redes sociais, empresas privadas e muitos outros, contudo, existe uma falta na temática de jogos digitais.

Então, em paralelo a isso foi feita também uma busca na BRAPCI pelo termo “jogos digitais” que trouxe 18 resultados, e após a análise foi identificado que apenas um artigo contempla as duas temáticas principais, Privacidade de Dados e Jogos Digitais.

O artigo em questão foi o “*DIO: um jogo em dispositivos móveis para mapear câmeras de vigilância | DIO: a mobile game to map surveillance cameras*” de autoria

de Rafael de Almeida Evangelista, Tiago Soares, Sarah Costa Schimidt e Felipe Lavignatti. Nesse artigo, os autores discutem a respeito de um jogo que na época estava em desenvolvimento cujo objetivo era utilizar das câmeras de celulares, e os dados gerados poderiam ser utilizados por empresas, tal como o *Pokemón Go*, lançado no mesmo ano. Eles pontuam que na sociedade contemporânea, as câmeras de vigilância são tecnologias de uso rápido e crescente. As razões dadas para essa proliferação estão principalmente relacionadas a preocupações com segurança. Nos países pobres, a ênfase está no controle da criminalidade urbana. Nos países ricos, elas são justificadas também pela ameaça do terrorismo. DIO é um jogo para celulares, ainda em desenvolvimento, que tematiza a proliferação das câmeras em áreas urbanas, promovendo um mapeamento colaborativo de sua localização geográfica. Os jogadores escolhem uma de duas equipes a quem se associam e desenvolvem as seguintes tarefas: 1) geolocalizar e fotografar câmeras de vigilância distribuídas pelas ruas; 2) competir com o outro time pelo controle das câmeras. As câmeras cadastradas então se transformam em pontos geolocalizados com os quais os jogadores interagem, com as câmeras sendo “capturadas” quando o jogador está fisicamente próximo a elas. Este artigo apresenta o enredo básico do jogo, suas regras e sua dinâmica. Também discute o uso econômico de dados pessoais, sua importância prevista no mercado mundial no futuro próximo e como tematizar essa questão fazendo uso de gamificação.

4 CONSIDERAÇÕES FINAIS

O trabalho de conclusão de curso em questão, procurou atender aos aspectos relevantes das principais normativas acerca do tema de segurança dos dados e do tema principal do trabalho, Aspectos da Biblioteconomia e Ciência da Informação para a privacidade de dados e ambientes digitais. Assim, foi considerado abranger as normativas que rodeiam o tema, como o MCI, a LGPD, a GDPR e a CF/88.

Percebe-se que dados se constituem como a menor unidade de informação gerados no ambiente informacional e, muitos dados gerados pela sociedade em geral, são comercializados e seguem para as empresas de marketing que realizam o tratamento desses dados, muitas vezes objetivando gerar lucros para o mercado.

É possível considerar que a privacidade é um conceito que ao longo dos anos ampliou seu significado. No contexto de segurança de dados e jogos eletrônicos, a privacidade ainda vem sendo muito discutida, a partir do momento em que se encontram cenários de aumento de processos judiciais sobre empresas que tratam os dados pessoais de maneira indevida, acarretando até mesmo no vazamento ou uso indevido de dados pessoais.

Por conta desses problemas, algumas leis foram criadas para a proteção e segurança não só dos dados, como também dos indivíduos, garantindo a privacidade dos usuários. Essas medidas de privacidade servem como meio de proteção para usuários e organização, visando o uso da rede de forma segura.

A partir do resultado do mapeamento, constata-se que um maior número de publicações relacionadas à privacidade de dados surge em períodos de dois anos após a data de implementação do Marco Civil e da LGPD (2016 e 2020), tornando o processo de disseminação da informação mais fácil e criando novas perspectivas de estudo a partir deles.

É visto também que o cenário brasileiro de publicações a respeito de privacidade digital é bastante amplo e abrange os mais diversos segmentos nessa temática.

Contudo, fica claro o quanto a temática de segurança e privacidade em jogos digitais ainda precisa ser estudada, e disseminada para a população no geral, o único artigo encontrado na BRAPCI juntando os dois temas, apesar de muito relevante, é

nichado e foca em um jogo específico. De 2016, ano da publicação, a 2022 as tecnologias e o acesso a elas já se aprimoraram em outro nível.

É nesse contexto que entram os jogos digitais, uma vez que a privacidade em jogos digitais envolve dados importantes dos usuários, como sua faixa etária, localização, etc. Porém, ainda com a coleta de informações importantes, na indústria de jogos já ocorreram invasões à rede, a exemplo da Sony, em 2011, além de supostos vazamentos de dados. A propaganda, por exemplo, é um bom exemplo disso, quando direcionada a usuários com determinados perfis e gostos para diferentes jogos.

Por isso, entende-se a privacidade como um direito fundamental de todo cidadão. No Brasil, as empresas ainda estão se adaptando às legislações acerca da privacidade, entre elas, a LGPD e a população estão começando a compreender o que significa a segurança dos dados e sua importância.

Verificou-se que muitas pessoas têm pouco conhecimento aprofundado sobre a lei de proteção aos dados, ao mesmo tempo, em que muitas delas se sentem invadidas ao oferecerem informações pessoais a um site ou rede.

Quanto às legislações, entre elas, a LGPD, essa cumpre seu papel de modo satisfatório e, seguindo em vigência, está fazendo com que progressivamente as pessoas tomem mais conhecimento sobre o tema e as empresas, maiores cuidados quanto aos dados pessoais de indivíduos e dados pessoais sensíveis.

Contudo, é evidente que ainda há muito a ser feito para tornar o cenário aceitável, em um país com índices educacionais tão baixos, uma série de fatores contribuem para que os cidadãos tenham seus direitos resguardados.

Cabe então ao Poder Legislativo brasileiro, propor políticas públicas com o intuito de informar à população a respeito das leis e dos seus direitos, paralelo a isso, empresas não devem somente tratar e proteger os dados dos seus usuários, mas também deixar mais claro que tipo de dados elas coletam e a finalidade disso. e por fim, a Autoridade Nacional de Proteção de Dados Pessoais (ANDP), deve cumprir seu papel de forma competente, fiscalizando a lei nº 13.709/2018 e garantindo a privacidade e a proteção de dados pessoais.

REFERÊNCIAS

ARAÚJO, C. A. A. Bibliometria: evolução histórica e questões atuais. **Em Questão**, Porto Alegre, v. 12, n. 1, p. 11–32, 2006. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/16. Acesso em: 28 jun. 2022.

AVILA, S. B.; GALLEGO, M. D.; NOYES, J. Uses and Gratifications on Augmented Reality Games: An Examination of Pokémon Go. **Applied Sciences**, v. 10 (5), n. 1644, 2020. Disponível em: https://www.researchgate.net/publication/339620307_Uses_and_Gratifications_on_Augmented_Reality_Games_An_Examination_of_Pokemon_Go. Acesso em: 10 mar. 2022.

AVILA, S. B.; GALLEGO, M. D.; NOYES, J. Uses and Gratifications on Augmented Reality Games: An Examination of Pokémon Go. **Applied Sciences**, v. 10 (5), n. 1644, 2020. Disponível em: https://www.researchgate.net/figure/Pokemon-Go-interfaces_fig1_339620307. Acesso em: 10 mar. 2022.

BASTOS, Athena. **Direito digital**: guia da lei geral de proteção de dados pessoais: LGPD. 2018. Disponível em: https://blog.sajadv.com.br/direito-digital-lei-de-protecaode-dados/. Acesso em: 01 set. 2022.

CASAROTO, Camila. A lei de dados agita empresas: veja aqui como se adequar à LGPD. **Rockcontent**. 2021. Disponível em: https://rockcontent.com/br/blog/lei-de-dados-agita-empresas/. Acesso em: 21 mar. 2022

BERNARDO, K. F.; SANTOS, A. S.; SANTOS JUNIOR, A.; BENTO, L. O. A vulnerabilidade do consumidor no uso da comunicação personalizada: dados versus invasão de privacidade. **Revista P2P e INOVAÇÃO**, v. 8, p. 93-110, 2021. Disponível em: https://brapci.inf.br/index.php/res/v/164620. Acesso em: 18 mar. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Centro Gráfico, 1988.

DALMASSO, Alexandre. **PIPEDA – A segunda Lei de Privacidade de Dados no Canadá**. 2020. Disponível em: https://alexandredalmasso.com/pipeda-a-segunda-lei-de-privacidade-de-dados-no-canada/. Acesso em: 20 de mar. 2022.

DALMASSO, Alexandre. ***Privacy Act* – a Primeira das Leis de Privacidade de Dados no Canadá**. 2020. Disponível em: https://alexandredalmasso.com/privacy-act-a-primeira-das-leis-de-privacidade-de-dados-no-canada/. Acesso em: 20 de mar. 2022.

Dhillon, G. (2004). Realizing benefits on an information security program. **Business Process Management Journal**, 10 (3), 260-261. Acesso em: 17 set. 2022

DIAS, G. A.; OLIVEIRA, B. M. J. F. de. Dados científicos: perspectivas e desafios. João Pessoa: Ed. **UFPB**, 2019.

EVANGELISTA, R. A.; SOARES, T.; SCHIMIDT, S. C.; LAVIGNATTI, F. Dio: um jogo em dispositivos móveis para mapear câmeras de vigilância | dio: a mobile game to map surveillance cameras. **Liinc em revista**, v. 12, n. 2, 2016. DOI: 10.18617/liinc.v12i2.913. Acesso em: 17 set. 2022.

GOOGLE. **Políticas de privacidade do Google**. [201-]. Disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/>. Acesso em: 31 ago. 2022.

JORGE, C. F. B.; OLIVEIRA, B. B.; MACHADO, J. G. C. F.; LIMA, M. S.; OTRE, M. A. C. Proteção de dados pessoais e covid-19: entre a inteligência epidemiológica no controle da pandemia e a vigilância digital. **Liinc em revista**, v. 16, 2020. Disponível em: https://brapci.inf.br/index.php/res/v/157434. Acesso em: 19 mar. 2022.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. **Computers & Security**, 28 (7), 493-508. Acesso em: 28 mar. 2022.

LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. **AtoZ: novas Práticas em Informação e Conhecimento**, v. 2, n. 1, p. 60-76, 2013. Disponível em: https://brapci.inf.br/index.php/res/v/15214. Acesso em: 10 mar. 2022.

MACHADO, C. E. M.; SANTUCHI, R. P.; CARLETTI, E. Z. B. O mercado de jogos eletrônicos e seus impactos na sociedade. **Multivix**, 2018. Disponível em: https://multivix.edu.br/wp-content/uploads/2018/08/o-mercado-de-jogos-eletronicos-e-seus-impactos-na-sociedade.pdf. Acesso em: 17 de mar. 2022.

MARCHIORI, P. Z.; LOPES, J. Princípios de informação equitativa nas políticas de privacidade online de empresas brasileiras. **Liinc em revista**, v. 12, n. 1, 2016. Disponível em: https://brapci.inf.br/index.php/res/v/93954. Acesso em: 19 jan. 2022.

OLIVEIRA, A. C. S.; ARAÚJO, D. S. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da lei geral de proteção de dados. **Liinc em revista**, v. 16, 2020. Disponível em: https://brapci.inf.br/index.php/res/v/157451. Acesso em: 12 fev. 2022.

PEREIRA, P. J. F. Segurança da informação digital. **Cadernos BAD (Portugual)**, n. 1, 2005. Disponível em: http://hdl.handle.net/20.500.11959/brapci/82222. Acesso em: 02 jun. 2022.

SANTOS, P. L. V. A. C.; SANT'ANA, R. C. G. Dado e Granularidade na perspectiva da Informação e Tecnologia: uma interpretação pela Ciência da Informação. **Ciência da Informação**, v. 42, n. 2, jan. 2013. Disponível em: http://revista.ibict.br/ciinf/article/view/1382/1560. Acesso em: 21 fev. 2020.

SETZER, Valdemar W. Dado, informação, conhecimento e competência. **DataGramaZero Revista de Ciência da Informaçã**o, n. 0, 2001.

SHINTAKU, M.; SOUSA, R. P. M.; COSTA, L. R.; MOURA, R. D. S.; MACEDO, D. J. Discussões sobre política de privacidade de dados em um sistema de informação governamental. **Em Questão**, v. 27, n. 4, p. 39-60, 2021. Disponível em: https://brapci.inf.br/index.php/res/v/162845. Acesso em: 22 jan. 2022.

SILVA, Rosane Leal; SILVA, Letícia Brum. A proteção jurídica de dados pessoais na internet: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. **Direito e novas tecnologias**. Florianópolis: FUNJAB, 2013. Disponível em: http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65. Acesso em: 31 ago. 2022.

SILVEIRA, S. A.; AVELINO, R.; SOUZA, J. A privacidade e o mercado de dados pessoais. **Liinc em revista**, v. 12, n. 2, 2016. Disponível em: http://revista.ibict.br/liinc/article/view/3719. Acesso em: 21 fev. 2021.

SOUSA, R. P. M.; BARRANCOS, J. E.; MAIA, M. E. Acesso à informação e ao tratamento de dados pessoais pelo poder público. **Informação & Sociedade: Estudos**, v. 29, n. 1, 2019. Disponível em: https://brapci.inf.br/index.php/res/v/111765. Acesso em: 09 mar. 2022

_____. As requisições de acesso aos dados do titular (DSAR). **AIQON**. 2020. Disponível em: https://aiqon.com.br/blog/as-requisicoes-de-acesso-aos-dados-do-titular-dsar/. Acesso em: 17 mar. 2022.

_____. Como a gamificação pode ajudar na segurança da informação?. **Ludos Pro**. [s.d.]. Disponível em: https://www.ludospro.com.br/blog/gamificacao-seguranca-da-informacao. Acesso em: 11 mar. 2022.

_____. Direitos dos titulares dos dados: Como lidar com as requisições. **AIQON**. 2020. Disponível em: https://aiqon.com.br/blog/direitos-dos-titulares-dos-dados-como-lidar-com-as-requisicoes/#:~:text=O%20DSAR%20%C3%A9%20uma%20forma,controlador%20de%20dados%20coletou%20dele. Acesso em: 17 mar. 2022.

_____. Em que pé estão as leis de proteção de dados no mundo. **Consumidor Moderno**. 2021. Disponível em: https://www.consumidormoderno.com.br/2021/02/08/em-que-pe-estao-as-leis-de-protecao-de-dados-no-mundo/. Acesso em: 18 mar. 2022.

_____. Games e dados: mecanismos jurídicos que devem ser observados. **Parceiro Legal**. 2019. Disponível em: https://parceirolegal.fcmlaw.com.br/lgdp/games-e-dados-mecanismos-juridicos/. Acesso em: 17 mar. 2022.

_____. O que é a CCPA, a lei de privacidade e proteção de dados da Califórnia? **Gatefy**. 2021. Disponível em: https://gatefy.com/pt-br/blog/o-que-e-ccpa-lei-privacidade-dados-california/. Acesso em: 17 mar. 2022.

_____. O uso de dados na indústria de games. **Ilumeo**. [s.d.]. Disponível em: https://ilumeo.com.br/todos-posts/2021/08/03/o-uso-de-dados-na-industria-de-

games#:~:text=A%20maioria%20das%20organiza%C3%A7%C3%B5es%20coleta,Cliente%2C%20Vendas%20e%20muito%20mais. Acesso em: 20 mar. 2022.

_____. Privacidade de dados no Japão. **AWS - Amazon Web Services**. 2022. Disponível em: https://aws.amazon.com/pt/compliance/japan-data-privacy/. Acesso em: 20 de mar. 2022.

_____. Segurança de dados é fonte de preocupação em games online. **FECOMERCIO-SP**. 2015. Disponível em: https://www.fecomercio.com.br/noticia/seguranca-de-dados-e-fonte-de-preocupacao-em-games-online. Acesso em: 28 fev. 2022.