



FACULDADE DE FILOSOFIA E CIÊNCIAS – Campus de Marília
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

JOSÉ ANTONIO MAURILIO MILAGRE DE OLIVEIRA

**A *BLOCKCHAIN* COMO CONTRIBUTO À TRANSPARÊNCIA E AUDITORIA
NOS PROCESSOS DE COMPARTILHAMENTO DE DADOS PESSOAIS**

Orientador: Professor Dr. José Eduardo Santarém Segundo

Marília-SP
2021

JOSÉ ANTONIO MAURILIO MILAGRE DE OLIVEIRA

***A BLOCKCHAIN COMO CONTRIBUTO À TRANSPARÊNCIA E AUDITORIA
NOS PROCESSOS DE COMPARTILHAMENTO DE DADOS PESSOAIS***

Tese apresentada ao Programa de Pós-Graduação em Ciência da Informação da Universidade Estadual Paulista Júlio Mesquita Filho como parte dos requisitos para obtenção do título de Doutor em Ciência da Informação.

Orientador: Prof. Dr. José Eduardo Santarém Segundo

Área de Concentração: Informação, Tecnologia e Conhecimento.

Linha de Pesquisa: Informação e Tecnologia.

Marília-SP

2021

ja.milagre@gmail.com

-
- M637a Milagre, José Antonio Maurilio
A blockchain como contributo à transparência e auditoria nos processos de compartilhamento de dados pessoais / José Antonio Maurilio Milagre de Oliveira. – Marília, 2021.
178 f. : il. ; 30 cm.
- Orientador: Prof. Dr. José Eduardo Santarém Segundo.
Tese (Doutorado em Ciência da Informação) – Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, 2021.
Bibliografia: f. 170-176.
1. Dados pessoais. 2. Privacidade. 3. Proteção de dados. 4. Blockchain. 5. Direitos. I. Santarém Segundo, José Eduardo (orientador). II. Título.

CDD 348.8

Ficha catalográfica elaborada por
Liliana Giusti Serra
CRB 8/5695

JOSÉ ANTONIO MAURILIO MILAGRE DE OLIVEIRA

**A *BLOCKCHAIN* COMO CONTRIBUTO À TRANSPARÊNCIA E AUDITORIA
NOS PROCESSOS DE COMPARTILHAMENTO DE DADOS PESSOAIS**

BANCA EXAMINADORA:

Prof. Dr. José Eduardo Santarém Segundo.

Instituição: Programa de Pós-Graduação em Ciência da Informação da UNESP/FFC

Prof. Dra. Angela Maria Grossi

Instituição: Programa de Pós-Graduação em Ciência da Informação da UNESP/FFC

Prof. Dr. Mario Furlaneto Neto

Instituição: Faculdade de Direito de Marília Fundação Eurípides Soares da Rocha

Prof. Dr. Clemilton Luis Bassetto

Instituição: Faculdades Integradas de Bauru

Prof. Dr. Cecílio Merlotti Rodas

Instituição: Programa de Pós-Graduação em Ciência da Informação da UNESP/FFC

Local: Universidade Estadual Paulista

Faculdade de Filosofia e Ciências

UNESP – Campus de Marília

Marília, 25 de março de 2021

*A Deus, porque ele é bom e seu amor dura para sempre.
A minha amada filha, Stephanie Milagre, por estar ao meu lado.*

AGRADECIMENTOS

Ao Professor Doutor José Eduardo Santarém Segundo.

Muito obrigado por confiar, sempre!

Aos professores membros da banca, Professora Doutora Angela Maria Grossi, Professor Doutor Mario Furlaneto Neto, Professor Doutor Cleminton Luis Bassetto e Professor Doutor Cecílio Merlotti Rodas, por ampliarem meu campo de visão sobre este estudo, com importantes contribuições. Obrigado!

MILAGRE, José Antonio Maurilio. **A Blockchain como contributo à transparência e auditoria nos processos de compartilhamento de dados**. Orientador: José Eduardo Santarém Segundo. 2020. 188 f. Tese (Doutorado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2021. Versões impressa e eletrônica.

RESUMO

As recentes regulamentações envolvendo dados pessoais estabelecem os direitos dos titulares dos dados e trazem importantes regras para os agentes de tratamento, incluindo o dever de legalidade, lealdade e transparência nas operações com dados pessoais. Dentre as operações com os dados pessoais, encontramos as transferências de dados como atividades constantes entre aplicativos, repositórios e redes sociais. Deste modo, a transferência ou compartilhamento de dados pessoais é prevista em ambientes digitais nas políticas de privacidade e proteção de dados, como forma de informar e aumentar a consciência do titular dos dados sobre as possibilidades existentes de compartilhamento. Apesar das declarações em políticas e termos, é necessário se investigar se o titular dos dados detém hoje o efetivo controle sobre transferências e compartilhamento de dados pessoais, se tem consciência das transferências que foram ou serão realizadas e se pode de forma transparente compreender e ver estes fluxos com seus dados pessoais. Neste ambiente, o objetivo desta tese é avaliar e demonstrar como o cenário de transferências de dados pessoais entre agentes de tratamento favorece o desconhecimento do titular de dados pessoais e constitui um risco para a privacidade e ameaça à proteção de dados pessoais. Neste sentido, desenvolveu-se a pesquisa de modo exploratório-descritivo e abordagem qualitativa. Avaliando-se as Legislações Brasileira e Europeia foram identificadas as melhores práticas relativas ao compartilhamento de dados e após, analisou-se cinco aplicações de Internet, populares no mundo, para verificar como disciplinam as questões relativas ao compartilhamento de dados. Conclui-se que as previsões sobre possibilidades de compartilhamento de dados em políticas e práticas não instrumentalizam de fato o direito do titular dos dados, dada a escuridão sobre as reais transferências que ocorrem, em que momento e por quanto tempo são realizadas. Apesar disso, o controle pleno do titular dos dados sobre as transferências e o efetivo exercício dos seus direitos pode ser aprimorado com a organização padronizada das informações relativas aos compartilhamentos, gravadas na *Blockchain*, permitindo-se a identificação e rápida visualização do rastreo das transferências de dados pessoais, garantindo-se aos titulares de dados a transparência prevista nos regulamentos e boas práticas.

Palavras-chave: Dados pessoais. Privacidade. Proteção de dados. Blockchain. Direitos.

ABSTRACT

The recent regulations involving personal data establish the rights of the data subjects and bring important rules for the processing agents, including the duty of legality, loyalty, and transparency in the operations with personal data. Among the operations with personal data, we find data transfers as constant activities between applications, repositories, and social networks. In this way, the transfer or sharing of personal data is provided for in digital environments in the privacy and data protection policies, as a way of informing and increasing the awareness of the data subject about the existing possibilities of sharing. Despite the statements in policies and terms, it is necessary to investigate whether the data subject currently has effective control over transfers and sharing of personal data, whether the holder of personal data is aware of the transfers that have been or will be made, and whether the holder can transparently understand and view these flows with his personal data. In this environment, the objective of this dissertation is to evaluate and demonstrate how the scenario of transfers of personal data between processing agents favors the ignorance of the holder of personal data and constitutes a risk to privacy and threatens the protection of personal data. In this sense, the research was developed in an exploratory-descriptive way and a qualitative approach, evaluating the Brazilian and European legislation, identifying best practices related to data sharing and then, analyzing five Internet applications, popular in the world, to see how they discipline data sharing issues. The dissertation concludes that the predictions about possibilities of data sharing in policies and practices do not really exploit the data subject's right, given the darkness about the actual transfers that occur, at what time and for how long they are carried out. Despite this, the full control of the data holder over transfers and the effective exercise of his rights can be improved with the standardized organization of information related to shares recorded on the blockchain, allowing the identification and quick visualization of the tracking of personal data transfers, ensuring to data subjects the transparency provided by regulations and best practices.

Keywords: Personal data. Privacy. Data protection. Blockchain. Rights.

LISTA DE FIGURAS

Figura 1: Formas de compartilhamento de dados e obrigações.....	65
Figura 2: Compartilhamento de dados para fins de análise (analytics).....	66
Figura 3: Workflow para requisição de compartilhamento de dados.....	68
Figura 4: Respeito ao princípio da prestação de contas no compartilhamento de dados	70
Figura 5: Meios comuns de compartilhamento de dados	84
Figura 6: Como o Facebook transfere os dados para prestar serviços globais	91
Figura 7: Dados de contato com Facebook	91
Figura 8: Contato feito com a rede social Facebook	92
Figura 9: Ferramenta Checkup de Privacidade	95
Figura 10: Exportação e Exclusão de Informações na plataforma Google.....	96
Figura 11: Opções que o titular de dados tem para obter informações sobre o Google	97
Figura 12: Apps com acesso à conta Google	98
Figura 13: Informações sobre os parceiros de publicidade Google	100
Figura 14: Formulário de contato WhatsApp	103
Figura 15: Link do botão para o e-mail de privacidade do WhatsApp.....	103
Figura 16: E-mail enviado ao WhatsApp	104
Figura 17: Resposta do WhatsApp sobre a solicitação das informações sobre o compartilhamento de dados pessoais	105
Figura 18: Tabela de Privacidade Strava.....	106
Figura 19: Página de Privacidade do Strava é inexistente.....	108
Figura 20: Página para contato prevista na política de privacidade da Samsung	110
Figura 21: Tecnologia Distribuída utilizada na Blockchain.....	118
Figura 22: Estrutura das redes Blockchains.....	122
Figura 23: Infraestrutura do AVOCATE	126
Figura 24: Arquitetura do Subject Contract Model	128
Figura 25: Diagrama do Subject Contract Model.....	129
Figura 26: Esquema pessoal de gestão e compartilhamento de dados em uma arquitetura-cliente servidor.....	133
Figura 27: Design de modelo de gestão de dados pessoais baseados na Blockchain	135
Figura 28: Modelo Conceitual para Rastreamento de Atividades de Compartilhamento de Dados Pessoais	155

LISTA DE QUADROS

Quadro 1: Dados, informação e conhecimento	37
Quadro 2: Dados inferidos a partir de dados fornecidos	39
Quadro 3: Dados, informação e conhecimento	42
Quadro 4: Quadro comparativo das atividades de tratamento de dados pessoais e fases do Ciclo de Vida dos Dados	44
Quadro 5: Comparativo entre a nomenclatura dos atores e agentes de tratamento de dados pessoais	50
Quadro 6: Descrição dos princípios-chave de proteção de dados	54
Quadro 7: ANEXO B - Modelo de Requerimento de Compartilhamento de Dados	72
Quadro 8: Anexo B – Modelo de formulário de decisão sobre compartilhamento de dados	73
Quadro 9: Informações para serem registradas sobre o compartilhamento de dados pessoais	74
Quadro 10: Avaliação dos Códigos e Práticas de Compartilhamento de Dados	87
Quadro 11: Avaliação da transparência das aplicações sobre compartilhamento de dados pessoais	112
Quadro 12: Política para envio de e-mails a cada 30 dias e configurações de Política para compartilhamento de dados com a finalidade de marketing do país “Itália”	130
Quadro 13: “A ledger” utilizado para autenticação, autorização e acesso	136
Quadro 14: Funcionalidades e elementos de funcionalidade de registros de atividades com dados pessoais	139
Quadro 15: Pesquisas revisadas	145

LISTA DE ABREVISATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
AC	Agente Controlador
AD	Agentes Diversos
AP	Agente Processador
API	<i>Application Programming Interface</i>
AT	Agente de Tratamento
CNIL	<i>Comission Nationale de l'Informatique et des Libertés</i>
CVD	Ciclo de Vida de Dados
Danfes	Documentos Auxiliares da Nota Fiscal Eletrônica
DLT	<i>Distributed Ledger Technology</i>
GDPR	<i>General Data Protection Regulation</i>
ICO	<i>Information Commissioner's Office</i>
IoT	Internet das Coisas
ID	Identidade
IP	<i>Internet protocol</i>
JSON	<i>JavaScript Object Notation</i>
KYC	<i>Know your customer</i>
LDW	<i>Linked Data Web</i>
LGPD	Lei Geral de Proteção de Dados
OWL	<i>Web Ontology Language</i>
P2P	<i>Peer-to-peer</i>
PDF	<i>Portable Document Format</i>
PDPC	<i>Personal Data Protection Commission</i>
PPGCI	Programa de Pós-Graduação em Ciência da Informação
RDF	<i>Resource Description Framework</i>
SIGILO	Associação de Defesa dos Titulares de Dados
SMTP	<i>Simple Mail Transfer Protocol</i>
TD	Titular de dados
TTPS	<i>Trusted Third Party</i>
UNESP	Universidade Estadual Paulista
XACML	<i>eXtensible Access Control Markup Language</i>

SUMÁRIO

1 INTRODUÇÃO.....	13
1.1 DEFINIÇÃO DO PROBLEMA DE PESQUISA.....	22
1.2 TESE, HIPÓTESE E PROPOSIÇÃO	23
1.3 OBJETIVOS	25
1.3.1 Objetivos específicos.....	26
1.4 MOTIVAÇÃO E JUSTIFICATIVA DA PESQUISA.....	26
1.5 PROCEDIMENTOS METODOLÓGICOS	29
1.6 ESTRUTURA DO TRABALHO	33
2 COMPARTILHAMENTO DE DADOS PESSOAIS, PROTEÇÃO DE DADOS E DIREITOS DOS TITULARES.....	36
2.1 DADOS PESSOAIS, ANONIMIZAÇÃO, PSEUDONIMIZAÇÃO E ATIVIDADES DE TRATAMENTO	36
2.2 ATORES ENVOLVIDOS NO TRATAMENTO DE DADOS PESSOAIS E A AUSÊNCIA DE TRANSPARÊNCIA	46
2.3 PRINCÍPIOS DO TRATAMENTO DE DADOS E APLICAÇÃO AO COMPARTILHAMENTO DE DADOS PESSOAIS	52
2.4 PREMISAS PARA TRATAMENTO DE DADOS PESSOAIS.....	56
2.5 O COMPARTILHAMENTO DE DADOS NAS LEGISLAÇÕES E OS DIREITOS DOS TITULARES DE DADOS	59
2.5.1 <i>General Data Protection Regulation</i>	59
2.5.2 Lei Geral de Proteção de Dados	61
2.5.3 Avaliação sobre os direitos trazidos envolvendo o compartilhamento de dados.....	62
3 CÓDIGOS DE PRÁTICAS E GUIDELINES DE PROTEÇÃO E COMPARTILHAMENTO DE DADOS	64
3.1 <i>Singapura Personal Data Protection Commission – Guide to Data Sharing</i>	64
3.2 <i>Data Sharing: A code of practice</i>	68
3.3 <i>Data Sharing code of practice (2020)</i>	70
3.4 <i>Guidance note: Template data sharing agreement and data processing agreement</i>	75
3.5 A ética do compartilhamento de dados: um guia para melhores práticas e governança.....	76
3.6 Código de Prática: Transmissão de dados aos parceiros para prospecção eletrônica: quais são os princípios a serem observados?.....	78
3.7 <i>Trusted Data Sharing Framework</i>	79
3.8 Avaliação regulamentos e dos códigos e boas práticas analisadas.....	82

4 AVALIAÇÃO DOS ASPECTOS COMPARTILHAMENTO DE DADOS EM APLICAÇÕES.....	89
4.1 CRITÉRIOS PARA A ESCOLHA DAS APLICAÇÕES.....	89
4.2 TERMOS DE USO DO <i>FACEBOOK</i>	89
4.3 POLÍTICA DE PRIVACIDADE DO <i>GOOGLE</i>	93
4.4 POLÍTICA DE PRIVACIDADE DO <i>WHATSAPP</i>	100
4.5 TERMOS DE USO <i>STRAVA</i>	105
4.6 POLÍTICA DE PRIVACIDADE <i>SAMSUNG</i> PARA <i>SMARTVS</i>	108
4.7 AVALIAÇÃO DA EXISTÊNCIA DE REGISTROS DE TRANSFERÊNCIA E DA TRANSPARÊNCIA OFERECIDA AO TITULAR DOS DADOS.....	110
5 A <i>BLOCKCHAIN</i> , DESCENTRALIZAÇÃO E DESAFIOS NA PROTEÇÃO A DADOS PESSOAIS.....	115
5.1 USO DA <i>BLOCKCHAIN</i> E ONTOLOGIAS PARA GESTÃO DO CONSENTIMENTO EM DISPOSITIVOS IoT.....	125
5.2 UMA PROPOSTA PARA TRANSPARÊNCIA E GESTÃO DE CONSENTIMENTOS.....	127
5.3 A <i>BLOCKCHAIN</i> COMO MECANISMO DE GARANTIA DE DIREITOS E OS REGISTROS IMUTÁVEIS.....	131
5.4 A <i>BLOCKCHAIN</i> PARA REGISTRO DE AUTORIZAÇÕES E <i>LOGGING</i> DAS ATIVIDADES.....	132
5.5 REQUISITOS E SISTEMAS PARA REGISTRO TRANSPARENTE DE <i>LOGS</i> DE ATIVIDADES ENVOLVENDO COMPARTILHAMENTO DE DADOS PESSOAIS.....	138
5.6 DISCUSSÃO SOBRE PONTOS OBSERVADOS NAS PESQUISAS SOBRE USO DA <i>BLOCKCHAIN</i> NO REGISTRO DE ATIVIDADES.....	141
6 UMA PROPOSTA PARA REGISTRO DESCENTRALIZADO DAS OPERAÇÕES DE COMPARTILHAMENTO DE DADOS PESSOAIS COM BASE NA <i>BLOCKCHAIN</i>	149
7 CONSIDERAÇÕES FINAIS.....	158
7.1 SUGESTÕES PARA TRABALHOS FUTUROS.....	167
REFERÊNCIAS.....	169

1 INTRODUÇÃO

Personal data is the new oil of the internet and the new currency of the digital world. (Meglena Kuneva, comissária para a Defesa do Consumidor, março 2009).

Novas Leis e Regulamentos surgem no mundo com o escopo de intensificar a proteção de dados de indivíduos. A *General Data Protection Regulation* (GDPR) foi editada na Europa e entrou em vigor em maio de 2018, trazendo uma série de direitos a titulares dos dados e deveres para os denominados agentes de tratamento, pessoas físicas e jurídicas que tratam dados pessoais na realização de suas atividades.

Do mesmo modo, no Brasil tem-se a edição da Lei Geral de Proteção de Dados (LGPD). A norma estabelece direitos e deveres dos titulares de dados e tornou-se aplicável em setembro de 2020. Dentre os direitos previstos nas novas regulamentações de proteção de dados, encontra-se o direito de o titular em ser informado acerca do compartilhamento de dados feito pelo controlador de dados pessoais e para qual finalidade.

Embora sejam regulamentos que trazem importantes direitos aos titulares de dados, não há, na atualidade, comprovação de que as empresas que realizam tratamento de dados pessoais implementem adequadamente todos os controles e cumpram as diretrizes da norma. Há grande discussão sobre os direitos relativos à privacidade no contexto da sociedade da informação.

A grande quantidade de dados coletados, somada à constante vigilância aplicada pela tecnologia, aumento da capacidade de armazenamento e a celeridade com que podem ser transferidos, são apontados como fatores da grande ameaça à privacidade dos indivíduos (MASON, 1986; TAVANI, 2008). O termo *Big Data* surge em 1997, na NASA, e foi designado para definir a condição de uma base de dados que, dado o seu volume, velocidade e variedade de dados, excede as capacidades técnicas e de infraestrutura para seu armazenamento, processamento e visualização (DUMBILL, 2012).

A transparência dos termos de uso e políticas de privacidade hoje são questionamentos realizados em debates públicos no escopo de exigir que a legislação, efetivamente, garanta a privacidade como um dos maiores direitos do indivíduo, isto porque o aproveitamento indevido da informação vem se tornando cada vez mais

frequente, o que demanda a necessidade de maior transparência das políticas de privacidade, que devem assegurar aos seus titulares a propriedade sobre seus dados (LOTT; CIANCONI, 2018).

Os dados coletados inserem-se em um contexto de *vigilância distribuída*, afirmada por BRUNO (2013) para descrever o atual cenário envolvendo a capacidade de coleta de dados pessoais, onde podemos identificar: a) uma vigilância descentralizada; b) diversidade tecnológica e de dispositivos de coleta de dados; c) indiscernibilidade inicial sobre o foco da vigilância; d) utilização potencial ou secundária de dispositivos que não foram desenvolvidos para fins de vigilância, com esta finalidade; e) análise feita por agentes humanos e não humanos; f) utilização das redes, notícias e compartilhamentos; g) participação e colaboração do meio social, de forma independente e não estruturada, por parte dos indivíduos conectados à rede.

Sistemas de geolocalização, sensores, sistemas de controle de trânsito, cartões magnéticos, sistemas *online*, sistemas em dispositivos conectados à Internet, mecanismos de busca, dentre outros, são algumas das ferramentas utilizadas para coleta de dados pessoais, em um ambiente onde, conforme descreveu Braman (2006), as informações são coletadas “por atacado”, de forma abrangente e sem distinção ou limite temporal.

Lott e Cianconni (2018) afirmam que a transparência dos termos de uso e políticas de privacidade dos serviços digitais envolvendo dados pessoais sensíveis vêm sendo questionados em muitos debates no sentido de exigir das legislações que efetivamente garantam a privacidade como um dos principais direitos dos indivíduos, sendo que o aproveitamento indevido de informações pessoais vem se tornando cada vez mais frequente.

Discussões científicas tratam do aproveitamento indevido de dados pessoais nas fases de coleta e armazenamento dos referidos dados, sendo considerada, inclusive, a possibilidade de coleta de dados pessoais de forma inconsciente por parte do titular dos dados pessoais. A coleta de dados e armazenamento de dados pessoais sem a participação ou o conhecimento do titular de dados é tema de pesquisas científicas. Affonso (2018) descreve que embora a abstração nas tecnologias da informação seja fundamental para redução da complexidade da interação do usuário em ambiente digitais, omitindo-se deste certos detalhes do processo, por outro lado perdendo o indivíduo a capacidade de compreender quais dados são coletados, tornando-se, conseqüentemente, mais difícil o conhecimento sobre os elementos presentes na fase de coleta de dados e as ações dos detentores, não havendo consciência do usuário sobre este processo.

Por outro lado, após a coleta, outra questão apresenta-se como não menos opaca aos titulares de dados: o compartilhamento. Não basta ao usuário ter conhecimento de quais dados são coletados, mas é relevante que saiba quais interfaces de recuperação de dados foram construídas e para quais outros agentes de tratamento os referidos dados foram compartilhados, pois não se pode controlar o que não se pode medir, não se gerencia o que não se mede, não se mede o que não se define, não se define o que não se entende, e não há sucesso no que não gerencia (DEMING apud AUDY, 2016).

O Ciclo de Vida de Dados (CVD) (SANT'ANA, 2013) representa a fase onde ocorre a transferência ou compartilhamento de dados pessoais, descrevendo-a como a fase de “recuperação”, sendo a fase onde se torna os dados disponíveis para acesso e uso e onde são pensadas estratégias e ações a partir do ponto de vista do responsável por sua manutenção, e onde a preocupação está com meios que ampliem os níveis de utilização destes dados via cópia ou obtenção de conjuntos para análise por meio de recursos de visualização dos dados (SANT'ANA, 2013).

Dentre as fases do ciclo de vida de dados, é importante destacar que a fase de recuperação é a fase destinada a criar-se mecanismos para que outros agentes de tratamento possam utilizar os referidos dados pessoais. Neste momento, pode-se indicar como a fase em que o compartilhamento de dados poderá acontecer, sem que o titular dos dados pessoais tenha consciência das referidas transferências de dados pessoais.

Esta dinâmica constitui-se em absoluto risco ao titular de dados pessoais, pois tão grave quando coletar ou armazenar, é compartilhar, vender, comercializar e lucrar com os bancos de dados pessoais, dados estes que foram cedidos para uma finalidade específica. A comercialização de dados pode inclusive ter a finalidade de análise de perfis de titulares de dados, por meio de algoritmos informatizados, para o oferecimento de propaganda direcionada.

Dados pessoais, conforme relatório do Fórum Econômico Mundial, podem ser classificados como as informações e metainformações criadas sobre as pessoas, abrangendo: a) dados oferecidos voluntariamente (como por exemplo, os perfis em redes sociais); b) dados observados (como por exemplo, dados de geolocalização e acessos Web); c) dados inferidos (como por exemplo, a análise de dados para uma pontuação de crédito) (WEF, 2011).

Silveira, Avelino e Souza (2016) informam que o mercado de dados pessoais compreende um ecossistema envolvendo atores humanos e não humanos, empresas,

plataformas, usuários, *data centers*, programas de rastreamento, bancos de dados, entre outros. O mercado pode ser classificado em quatro camadas, sendo elas:

- a) Coleta e armazenamento de dados;
- b) Processamento e mineração de dados;
- c) Análise e formação de amostras;
- d) Modulação.

Na fase de coleta e armazenamento de dados, estariam presentes as vendedoras, *brokers* e coletoras de dados para empresas de publicidade e *marketing* (SILVEIRA; AVELINO; SOUZA, 2016). É na fase de modulação onde ocorreria a atuação dos algoritmos de controle de visualização e formação de bolhas e “*clusters*” de consumidores. Existem empresas que são especializadas em coleta de dados, denominados “dados observados”, com compartilhamento remunerado a outras empresas.

Neste sentido, o compartilhamento de dados pode ser utilizado para correlação com outras bases de dados, para extração de resultados, sem que o titular tenha conhecimento destas operações, o que pode resultar em ameaças à privacidade, no que Mason (1986) classifica como o acréscimo de atributos inerente às conjunções entre dados cedidos a entidades diferentes e que quanto mais atributos são adicionados, maiores os danos ocorrem à privacidade.

Outro risco grave está ligado à classificação dos titulares de acordo com seus dados. Pariser (2011) descreve como “*filter bubble*”, os algoritmos dispostos em locais da Web, redes sociais e *sites*, que selecionam informações que um titular de dados gostaria de ver, com base em dados coletados anteriormente, relacionados com outras informações.

Os prejuízos inerentes ao compartilhamento indevido de dados pessoais podem ser constatados, como no identificado na matéria do jornal *The Guardian*, que abordou a cessão indevida de dados pessoais do *Facebook* à *Cambridge Analytica*, para campanhas eleitorais. A empresa de análise de dados que trabalhou para o time eleitoral de Donald Trump e venceu a campanha do Brexit coletou milhões de dados de perfis de eleitores americanos, em um dos maiores vazamentos de dados na área de tecnologia, dados que foram usados para a construção de um poderoso programa de computador para prever e influenciar escolhas eleitorais. Os dados foram coletados por meio de um aplicativo denominado *thisisyourdigitalife*, desenvolvido pelo acadêmico Aleksandr Kogan, onde centenas de milhares de usuários foram pagos para realizar o teste de personalidade *online*

e concordaram em ceder seus dados para fins acadêmicos (CADWALLADR; GRAHAM-HARRISON, 2018).

O caso elenca um evidente problema de auditoria das operações de compartilhamento de dados pessoais, considerando que o *Facebook* negou que a coleta de dezena de milhões de dados pessoais pela *Cambridge Analytica* tenha sido uma violação de dados pessoais, informando que a empresa obteve acesso aos dados de maneira legítima, mas não seguiu as regras posteriormente, considerando que passou os dados a terceiros (CADWALLADR; GRAHAM-HARRISON, 2018).

Isaac e Hanna (2018) explicam que a onipresença da coleta, armazenamento, análises de equipamentos, plataformas, sistemas, aplicativos e plataformas de mídias sociais destinadas a personalizar experiências, otimizar vendas e maximizar o retorno foram perturbadoras na formação da economia global, no fluxo de ideias e no acesso a informações que resultaram no avanço da inovação. Este risco é ainda mais exacerbado pelo fato de dispositivos de Internet das Coisas (IoT) estarem se tornando mais integrados em sistemas maiores que governam todos os aspectos de nossas vidas. Para Barker (2014), pesquisas indicam que em 2020 a quantidade de objetos interconectados superaria os 25 bilhões.

Conforme a *Federal Trade Commission* (2015), IoT refere-se a objetos físicos interconectados com a Internet, como computadores, sensores e objetos, interagindo entre si e realizando o tratamento de dados no contexto de hiper conectividade (FTC, 2015 *apud* MAGRANI; OLIVEIRA, 2019, p. 81).

Dispositivos inteligentes conectados na Internet, auxiliando pessoas em diversas atividades, podem representar benefícios da tecnologia. Por outro lado, revelam a necessidade de uma reflexão sobre os riscos do tratamento indevido de dados pessoais, a partir destes mesmos dispositivos, graças a sua opacidade, confundindo o titular de dados, impedindo que este realmente tenha dimensão do que é tratado a respeito, antes de consentir, fragilizando o direito de consentimento, que não se manifesta como a Lei prevê, de forma livre, expressa, informada e inequívoca, e expondo a necessidade de outras formas de proteção do titular de dados.

No entanto, o uso da tecnologia requer atenção especial para proteção dos direitos dos usuários, pois podem oferecer riscos à privacidade e segurança, considerando ainda que em um cenário em que indivíduos não tem conhecimento sobre o que estão autorizando, diante de termos ambíguos, de linguagem técnica e com omissões de informações, o modelo de consentimento falho e ineficaz não deve ser encarado como

principal forma de uso de dados, sobretudo no cenário de IoT, sendo o *privacy by design* uma ferramenta a ser considerada (MAGRANI; OLIVEIRA, 2019, p.82).

Em 2013 pesquisadores do Centro de Psicometria da Universidade de Cambridge analisaram os resultados de voluntários que fizeram um teste de personalidade no *Facebook* para avaliar seu perfil psicológico “OCEAN” (abertura, consciência, extroversão, agradabilidade e neuroticismo) e o correlacionaram com suas atividades do *Facebook* (curtidas e compartilhamentos). A pesquisa reuniu 350.000 participantes nos EUA e estabeleceu uma relação clara entre a atividade do *Facebook* (e outros indicadores *online*) e esse perfil de personalidade com cinco fatores, sendo possível demonstrar que o perfil OCEAN pode ser deduzido com razoável precisão para qualquer indivíduo da rede social, observando essas métricas e sem usar um instrumento psicográfico formal (ISAAC; HANNA, 2018).

A descoberta de que o *Facebook* concedeu acesso irrestrito a mais de 87 milhões de dados pessoais para a *Cambridge Analítica* aumentou sensivelmente o debate sobre o impacto e riscos da tecnologia na privacidade e sobre as garantias dos cidadãos acerca do compartilhamento de seus dados.

Um outro exemplo é a parceria entre a rede social *Facebook* e *Experian*, permitindo a segmentação de *posts* a partir da renda individual e familiar e outros dados coletados por estas empresas de crédito. A parceria foi extinta em 2018 após o escândalo da *Cambridge Analítica*. O mesmo acontecendo com o aplicativo *Waze*, onde o *Facebook* permitia anúncios de empresas direcionados às pessoas que estão próximas da localidade da empresa.

Erros e falhas no compartilhamento de dados pessoais também constituem riscos graves a titulares e dados. Uma falha humana de um cientista de dados do Hospital Albert Einstein, que compartilhou dados pessoais em uma plataforma usada por programadores, expôs dados de 16 milhões de pacientes que já passaram por algum tratamento ou teste relacionado à COVID-19 (PRASER, 2020). No entanto, nem todas as falhas se tornam de conhecimento público, e muitas são ocultadas pelos controladores de dados.

Como se pode constatar, conforme Gerd Leonhad (2018, *apud* NUNES, 2018), dados pessoais são o novo petróleo da humanidade, e existe real preocupação sobre o compartilhamento remunerado e desconhecido pelo próprio titular, além da necessidade de se avisar ao titular de dados, rapidamente, sempre que uma transferência se mostrar insegura ou apresentar falhas.

Considerando o atual cenário e a dificuldade entre identificar se os agentes de tratamento estão cumprindo ou não as disposições relativas a proteção de dados pessoais, no que diz respeito ao compartilhamento de dados, foi realizada a pesquisa no escopo de responder as seguintes questões: Como o compartilhamento de dados pessoais entre agentes de tratamento pode ser comprovado e quais os controles disponíveis aos titulares de dados pessoais para visualizar os fluxos realizados com seus dados pessoais?

É na fase de recuperação de dados que se estabelece a preocupação com o fator privacidade nesta pesquisa, tendo-se em vista que os titulares de dados pessoais devem ser considerados, devendo haver a previsão de associação de dados recuperados com outros dados, o que pode constituir um ataque, do mesmo modo, deve ser possível identificar as estruturas de transferência de dados, sendo igualmente, no elemento disseminação, relevante que seja claro que os usuários sejam informados sobre a disponibilização dos dados:

Quando se trata de dados sensíveis, os usuários tendem a ter identificação forte e com direitos restritos de acesso, mas, mesmo assim, estes usuários precisam receber a informação de que aquele dado está disponível (SANT'ANA, 2016, p. 134).

Por outro lado, existe uma sensível diferença entre a informação ao usuário, por meio de termos, políticas e avisos e comprovação para o usuário sobre o que realmente é feito com seus dados pessoais. Não basta receber a informação, pois as novas regulamentações asseguram a transparência para o titular de dados em conhecer quais os fluxos sendo feitos com seus dados pessoais. Como adverte Silveira, Avelino e Souza (2016, p. 228):

Tudo indica que uso massivo de dados pessoais terá efeitos ambivalentes em nossa sociedade. O cenário atual permite afirmar que o mercado de dados dará maior poder às corporações do que aos cidadãos em relação às trocas que realizam. [...] A pesquisa aqui relatada está em sua fase inicial, mas indica a existência de uma economia da intrusão e da interceptação de dados pessoais que clama pela transparência completa do cotidiano das pessoas diante do interesse econômico das forças do mercado.

As menções a compartilhamento de dados pessoais em políticas de privacidade aparentemente não revelam claramente as intenções para com os dados do titular e normalmente estão relacionadas à justificativa de oferecimento de produtos e serviços personalizados. Um exemplo pode ser visto na política da privacidade da *Samsung*:

A *Samsung* divulga as informações do Cliente internamente, mas apenas aos destinatários que necessitem de ter conhecimento das mesmas de modo a fornecer os Serviços, para dar resposta aos pedidos do Cliente.

A *Samsung* também divulgará as informações do Cliente às seguintes entidades, mas apenas na medida em que tal seja necessário para fornecer os Serviços da *Samsung*:

Afiladas:

Outras empresas do grupo *Samsung Electronics* que a *Samsung* controla ou detém.

Parceiros de Negócio:

Parceiros com os quais a *Samsung* trabalha para fornecer ao Cliente os Serviços que este último pediu ou comprou. Por exemplo, a *Samsung* poderá trabalhar com um banco para que o Cliente possa utilizar um dos Serviços da *Samsung* para efetuar pagamentos mais rápidos e mais eficientes. Estes parceiros de negócio controlam e gerem as informações pessoais do Cliente.

Fornecedores de Serviços:

Empresas cuidadosamente selecionadas, que prestam serviços para ou em nome da *Samsung*, tais como empresas que prestam serviços de reparações, centros de contacto ao cliente, atividades de atendimento ao cliente, publicidade (incluindo publicidade personalizada nos *Websites* da *Samsung*, *Websites* de terceiros, ou em plataformas *online*), realização de inquéritos de satisfação dos clientes, ou faturação, ou que enviam *e-mails* em nome da *Samsung*. Estes fornecedores estão também empenhados em proteger as informações do Cliente.

Outras Entidades, quando Exigido por Lei, ou conforme Necessário para Proteger os Serviços da Samsung:

Por exemplo, pode ser necessário nos termos da lei, de processos legais jurídicos ou por ordem emitida por autoridades governamentais ou administrativas divulgar as informações do Cliente. Estas Entidades poderão também solicitar à *Samsung* informações por motivos de aplicação da lei, de segurança nacional, de combate ao terrorismo, ou por outros motivos relacionados com a segurança pública.

Outras Entidades Relativamente a Transações Empresariais:

A *Samsung* poderá divulgar as informações do Cliente a terceiros no âmbito de uma fusão ou transmissão, aquisição ou venda, ou em caso de insolvência.

Outras Entidades com a Autorização do Cliente, ou com a Orientação do Cliente:

Para além das indicações descritas nesta Política de Privacidade, a *Samsung* poderá partilhar informações sobre o Cliente com terceiros quando o Cliente autorizar ou solicitar tal partilha, em separado (SAMSUNG, 2020, p. 1).

Por sua vez, o comunicador instantâneo *WhatsApp*, informa em sua política de privacidade os dados do titular que partilha, no entanto, não assegura qualquer benefício na utilização da plataforma como justificativa, e do mesmo modo, não informa quais são os agentes de tratamento que receberão dos dados:

Seus dados são compartilhados à medida que você utiliza e se comunica usando nossos Serviços e nós compartilhamos seus dados para nos ajudar a operar, aprimorar, entender, personalizar, dar suporte e a promover nossos Serviços.

- **Dados da conta.** Seu número de telefone, seu nome e foto do perfil, seu *status online* e mensagem de *status*, o *status* de visto pela última vez e as notificações de entrega podem estar disponíveis para qualquer um que utilize nossos Serviços; no entanto, é possível configurar os Serviços para definir se alguns dados devem ficar disponíveis para outros usuários.
- **Seus contatos e outros.** Os usuários com quem você se comunica podem armazenar ou compartilhar seus dados (inclusive seu número de telefone ou mensagens) com outras pessoas dentro e fora de nossos Serviços. É possível utilizar a configuração e o recurso de bloqueio em nossos Serviços para

gerenciar os usuários de nossos Serviços com quem você se comunica e a forma de compartilhamento de determinados dados.

- **Prestadores de serviço terceirizados.** Trabalhamos com prestadores de serviço terceirizados para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços. Quando compartilhamos dados com prestadores de serviço terceirizados, exigimos que eles utilizem seus dados de acordo com nossas instruções e termos ou mediante seu consentimento expresso.
- **Serviços de terceiros.** Quando você usa serviços de terceiros que são integrados aos nossos Serviços, eles podem receber dados sobre seus compartilhamentos. Por exemplo, ao usar um serviço de *backup* de dados integrado aos nossos Serviços (como o *iCloud* ou o *Google Drive*), eles receberão informações sobre o que é compartilhado por você. Ao interagir com um serviço de terceiros conectado com nossos Serviços, você pode acabar fornecendo dados diretamente a eles. Observe que ao usar serviços de terceiros, os termos e as políticas de privacidade aplicáveis serão os elaborados para tais serviços (WHATSAPP, 2020, p. 1).

A Lei Geral de Proteção de Dados (LGPD) estabelece que o titular tem direito de ter a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (BRASIL, 2018). No entanto, como se verifica, as empresas não atendem as determinações da nova Legislação, o que gera uma assimetria informacional.

Conforme Jensen e Meckling (1976), ocorre a assimetria informacional quando a relação entre o agente e o principal é conflitante, caracterizando-se quando os agentes estabelecem transações nas quais detêm informações quantitativas ou qualitativas superiores às demais partes envolvidas.

Pesquisa realizada pela Associação de Defesa dos Titulares de Dados (SIGILO), publicada em dezembro de 2020, estimou que 85% das empresas ignoram questionamentos sobre tratamento de dados. (LGPD, 2020).

A assimetria informacional pode ser reduzida por meio da organização da informação relativa à transferência de dados pessoais. A tecnologia *Blockchain* vem crescendo como poderoso instrumento de registro de transações em criptomoedas. No entanto, sua capacidade excede o registro apenas de transações com ativos digitais. Como estabelece Formigoni, Braga e Leal (2017), pode-se dizer que se trata de um sistema distribuído de base de dados em *log*, mantido e gerido de forma compartilhada e descentralizada (através de uma rede *peer-to-peer*, P2P), na qual todos os participantes são responsáveis por armazenar e manter a base de dados. As características da *Blockchain* são: segurança das operações, descentralização de armazenamento e de computação, integridade de dados e imutabilidade das transações.

Implantando-se o *Blockchain*, percebeu-se seu potencial e características, como imutabilidade, resiliência e inviolabilidade. Essas características permitem que a tecnologia possa ser pensada para outras finalidades, incluindo o registro de contratos inteligentes, os *Smart Contracts*. O próprio nome da tecnologia, está intimamente ligado com a forma em que armazena os dados, em “blocos”, anexados a uma cadeia, denominada “*chain*”.

Deste modo, realizou-se pesquisa exploratória em aplicações populares no Brasil, para primeiro identificar se os mesmos serviços *online* asseguram, nas políticas, os direitos relativos a compartilhamento de dados pessoais e se são claros a respeito de como e quando compartilham os dados. Após, identificou-se se é possível comprovar e identificar quais dados são transferidos e qual a participação do titular de dados pessoais no conhecimento e ciência sobre as operações de transferência de dados, inicialmente cedidos para uma finalidade específica, analisando-se igualmente a pesquisa científica que trata da *Blockchain* para o registro de atividades envolvendo dados pessoais. Por fim, apresentou-se uma proposta, com base na *Blockchain*, para registros descentralizados das operações de compartilhamento de dados.

Em tal ambiente, considerando a problemática envolvendo os processos de transferência e compartilhamento de dados, e o não conhecimento, por parte do titular dos dados das transferências realizadas e para quais atores, que se apresenta o problema, a tese, a hipótese, os objetivos, a justificativa, a delimitação do tema e a metodologia de pesquisa.

1.1 DEFINIÇÃO DO PROBLEMA DE PESQUISA

O compartilhamento de dados é uma das atividades dos agentes de tratamento, por meio do qual transferem os referidos dados a terceiros. No entanto, para o titular dos dados, não é claro conhecer quais os fluxos são feitos com referidos dados, não lhe sendo dado o direito de conhecer as atividades de compartilhamento.

Uma pesquisa realizada no final de 2018 pela *Privacy International* descobriu que vários aplicativos populares para *Android* – incluindo *Spotify*, *Duolingo* e *TripAdvisor* – transferiam automaticamente dados pessoais para o *Facebook* no momento que os usuários abriam o aplicativo, sem o consentimento do usuário. Eles descobriram que isso ocorreu mesmo que o usuário não tivesse uma conta no *Facebook*. A entidade conduziu uma investigação jurídica desse compartilhamento de dados e identificou que os

aplicativos ficaram abaixo de um padrão aceitável em relação ao consentimento e à privacidade do usuário sob a *General Data Protection Regulation* e *ePrivacy* Diretiva. As pessoas estão perdendo rapidamente a confiança na capacidade do *Facebook* de manter informações seguras, já que nos últimos anos a gigante da tecnologia, que tem mais de 2 bilhões de usuários ativos em todo o mundo, ganhou a atenção de uma série de violações de dados e vulnerabilidades de privacidade, o que fez com que pessoas deixassem a plataforma. No entanto, pesquisas recentes da Universidade de Oxford sugeriram que o *Facebook* ainda pode rastrear informações sobre pessoas que nem sequer possuem contas na rede, por meio de rastreamento de terceiros em aplicativos móveis. A *Privacy International* descobriu que mais de 60% dos aplicativos *Android* em seu estudo compartilharam dados com o *Facebook* no momento em que um usuário abriu o aplicativo, independentemente de o usuário estar conectado ao *Facebook* ou ter uma conta no *Facebook* (CHUEN, 2019).

Neste contexto, o desconhecimento do titular dos dados pessoais acerca do caminho pelo qual seus dados percorrem após o seu fornecimento a determinados agentes de tratamento pode expor sensivelmente sua privacidade, financiar o mercado de dados pessoais e vem em sentido oposto aos regulamentos de proteção de dados pessoais. Embora os agentes de tratamento implementem em políticas previsões sobre o compartilhamento de dados, estes não apresentam transparência nas operações de tratamento realizadas e com quais agentes compartilham os referidos dados, ou quando o compartilhamento ocorreu.

A partir desta premissa, faz-se assim o entorno do **problema de pesquisa**: É possível reduzir esta flagrante assimetria informacional a partir do uso da tecnologia *Blockchain*, com o registro descentralizado das operações de compartilhamento de dados?

1.2 TESE, HIPÓTESE E PROPOSIÇÃO

A tecnologia *Blockchain* vem se apresentando como ferramenta que reúne importantes características para o rastreamento de ativos, sendo considerada uma *Distributed Ledger Technology* (DLT). Para Ferreira (2017), o grande segredo para a consolidação dessa tecnologia é a cooperação. Neste contexto, as DLT's oferecem uma solução que possibilitam a rastreabilidade, segurança e até uma medição das trocas de conhecimento ocorridas na rede.

Neste sentido, a **tese** desta pesquisa é que a assimetria informacional existente entre o titular de dados pessoais e os agentes de tratamento de dados, especificamente no que tange ao compartilhamento de dados pessoais, pode ser reduzida por meio de um sistema autônomo, descentralizado, indelével e independente, que registre de forma segura as operações de compartilhamento de dados.

As normas de proteção de dados Pessoais que serão estudadas, Lei Geral de Proteção de Dados e *General Data Protection Regulation*, asseguram princípios (direitos fundamentais assegurados aos titulares de dados), que devem ser respeitados nas atividades envolvendo compartilhamento de dados e é neste ambiente que medidas de organização e recuperação das informações podem ser aplicadas para aprimorar a privacidade do titular de dados, como pode-se analisar nos princípios trazidos pelas normas:

- a) **Livre acesso, previsto na LGPD.** A consulta sobre a forma de tratamento deve envolver necessariamente o acesso às operações de compartilhamento realizadas. A descrição de dados e metadados para que titulares possam visualizar as operações é fundamental;
- b) **Transparência, previsto na LGPD.** O acesso aos registros de compartilhamento de dados pessoais deve ser facilmente acessível, claro, incluindo dados sobre todos os agentes de tratamento que trataram os dados. Estratégias de recuperação de dados podem cooperar com práticas de acessibilidade e encontrabilidade da informação, na construção dos sistemas que registrem as atividades de tratamento;
- c) **Responsabilização e prestação de contas, previsto na LGPD.** Os agentes devem provar a eficácia do cumprimento das obrigações legais, o que impõe um sistema descentralizado que registre o compartilhamento de dados e impeça ocultações e usos indevidos. A arquitetura de um sistema de organização informacional que não permaneça em posse do controlador e que não permita violações a dados pessoais, demonstra-se fundamental.
- d) **Licitude, lealdade e transparência, previsto na GDPR.** A transparência e lealdade, no que diz respeito ao compartilhamento de dados pessoais, só serão atendidas se os sistemas e operações puderem ser consultadas pelos titulares de dados. A utilização de princípios de publicação de dados para que o titular tenha possibilidade de realizar consultas rápidas, ao mesmo

tempo preservando sua privacidade, pode diminuir a distância informacional entre ele e as operações que são feitas com seus dados.

Busca a tese apresentar como a organização das informações sobre compartilhamento de dados pessoais poderá atender aos princípios e boas práticas legislativas e proporcionar a titulares a recuperação de informações sobre o que é feito com seus dados pessoais, cumprindo importante papel no desenvolvimento econômico, científico e social da sociedade.

Tem-se como **hipótese** que a utilização da tecnologia *Blockchain* poderá ser utilizada para registro de metadados relativos às operações de compartilhamento de dados, podendo ser auditada, analisada, ampliando ao titular o direito de conhecer os agentes de tratamento que receberam seus dados, a partir da interação com um único agente de tratamento.

Para tanto, **propõe-se**, a realização de estudo envolvendo a operação de tratamento denominada compartilhamento de dados pessoais, identificando-se:

- a) quais os direitos trazidos aos titulares de dados no que tange ao compartilhamento de dados, na legislação brasileira e europeia;
- b) quais os entendimentos e práticas recomendados por entidades e autoridades de proteção de dados para o compartilhamento e, a partir deste estudo;
- c) avaliar aspectos do compartilhamento de dados em aplicações, inspecionando se informam os agentes de tratamento, ou não, com os quais compartilham dados, para se apresentar, posteriormente;
- d) como a tecnologia *Blockchain*, a partir da revisão bibliográfica produzida, poderá contribuir na organização e recuperação de informações, no rastreamento das operações de compartilhamento de dados pessoais, identificando-se pontos de consenso entre as pesquisas, para, ao final;
- e) apresentar uma proposição de um modelo conceitual para registro de operações de compartilhamento, descentralizada, indelével e aditável.

1.3 OBJETIVOS

A proposição de um modelo conceitual para descrição, registro e recuperação das operações de compartilhamento de dados na *Blockchain*, a partir da caracterização da grave violação à privacidade decorrente da assimetria informacional sobre as reais

operações de compartilhamento de dados realizadas por agentes de tratamento de dados pessoais.

1.3.1 Objetivos específicos

- Identificar o conceito de “compartilhamento de dados” no Ciclo de Vida dos Dados;
- Avaliar quais os direitos trazidos aos titulares de dados pessoais na Lei Geral de Proteção de Dados e *General Data Protection Regulation*;
- Identificar guias, procedimentos e códigos de prática envolvendo compartilhamento de dados pessoais;
- Avaliar como o compartilhamento de dados pessoais vem sendo descrito nas Políticas de Privacidade e se contemplam a transparência mínima sobre descrição dos fluxos de dados, bem como se as aplicações estão atendendo requerimentos a respeito de informações sobre com quais entidades compartilham dados;
- Identificar quais os riscos à privacidade e para o exercício dos seus direitos decorrentes da opacidade do titular em conhecer as operações de compartilhamento dos seus dados;
- Caracterizar o ambiente da pesquisa envolvendo *Blockchain* e o registro de transações;
- Propor um modelo de organização e recuperação das informações relativas ao compartilhamento de dados pessoais, proporcionando transparência ao titular de dados no acesso às operações de compartilhamento de seus dados.

1.4 MOTIVAÇÃO E JUSTIFICATIVA DA PESQUISA

A motivação da pesquisa se dá pela identificação de ausência de transparência nos processos de compartilhamento de dados pessoais realizados por agentes de tratamento de dados, o que pode se caracterizar pela falta de propostas e modelos que possam servir de padrão para organização e recuperação destas informações.

Fica evidenciado que a privacidade ganhou contexto de absoluta relevância, sobretudo com o advento das normas de proteção de dados. Fica notório que saber para onde os dados fluem é questão relevante, um direito fundamental. Os regulamentos Europeu e Brasileiro asseguram a transparência como um dos direitos dos titulares de

dados pessoais. No entanto, não é possível assegurar ao titular de dados conhecimento sobre as operações de compartilhamento realmente feitas pelos agentes de tratamento de dados, pois não se tem a organização das informações destes processos, cada agente operando de forma diferente do outro. Os agentes de tratamento registram informações em suas políticas sobre o compartilhamento de dados, no entanto, não se apresentam dados suficientes para que o usuário conheça para onde seus dados são enviados a partir da coleta.

Este cenário patrocina o compartilhamento oculto de dados, alimentando uma indústria, como no caso envolvendo a rede social *Facebook*. Duzentos e sessenta e sete (267) milhões de dados de perfis do *Facebook* estavam, em abril de 2020, sendo comercializados na *Darkweb*, por U\$\$ 600,00. As vítimas eram, em sua maioria, dos Estados Unidos e tiveram nomes completos, números de telefone e códigos de identificação expostos, incluindo data de aniversário e gênero. Estes ataques motivaram campanhas de *phishing scam* direcionados (*spear phishing*) às pessoas que tiveram os dados comprometidos. Não se sabe exatamente como os dados foram obtidos, mas não se exclui a possibilidade de que eles foram roubados a partir de API (*Application Programming Interface*) desenvolvida, que permitia acesso a dados pessoais (HIGA, 2020).

Como se constata, se o vazamento não fosse descoberto, os titulares jamais descobririam quem teve acesso a seus dados pessoais e de que forma foram compartilhados.

No Brasil, o Ministério Público do Distrito Federal conseguiu judicialmente uma ordem para que a SERASA parasse de comercializar dados pessoais, com base na Lei Geral de Proteção de Dados. Estima-se que a SERASA comercialize dados pessoais de 150 milhões de brasileiros (MPDFT, 2020).

A assimetria informacional entre controladores e titulares é flagrante e atuação judicial ocorre quando se toma conhecimento. Mas nem todos os casos são conhecidos. É neste escopo que a pesquisa se apresenta, no sentido de contribuir para aprimoramento da privacidade dos titulares de dados, proporcionando o resgate da assimetria existente, sobretudo, diante da omissão das reais atividades de compartilhamento, organizando o emprego das tecnologias existentes.

Novas tecnologias engendraram novas oportunidades de acesso, criação, preservação disseminação e uso da informação. No entanto, é a atividade humana que permite que a informação seja transformada em conhecimento e, ainda, que esse conhecimento agregue valor à experiência e ao desenvolvimento humano. É o conhecimento que empodera as pessoas para

que melhorem seus meios de subsistência e contribuam com o desenvolvimento social e econômico das sociedades em que vivem (UNESCO, 2015, p. 30).

Com efeito, a importância da Ciência da Informação é notada como elemento capaz de lidar com os diversos elementos vinculados às novas tecnologias e o risco às pessoas.

Assim, os elementos vinculados à tecnologia passam a ser uma preocupação da Ciência da Informação, portanto, essa ciência pode amparar, por meio de estudos e pesquisas, os aspectos vinculados desde a coleta até a recuperação de dados, contribuindo para novas descobertas em relação à proteção de dados pessoais (AFFONSO, 2018).

Compreende-se a presente pesquisa no contexto dos processos de recuperação e organização da Informação. Conforme o Programa de Pós-Graduação em Ciência da Informação da Universidade Estadual Paulista (UNESP, 2019, p. 3):

A Ciência da Informação, enquanto área de conhecimento, encontra seu objeto de estudo nos processos relativos a produção, organização, gestão, mediação, apropriação, uso e recuperação da informação, utilizando-se de aportes interdisciplinares oriundos de áreas como a Ciência da Computação, a Linguística, a Comunicação, as Ciências Cognitivas, a Psicologia, a Matemática, a Lógica, a Administração, a Educação, a Sociologia, a História e a Diplomática, entre outras, seja para melhor explicar tais processos, seja para aquilatar o seu impacto nos fazeres das distintas ambiências informacionais.

E a invasão da tecnologia na sociedade aclara necessidade de as pessoas entenderem os aspectos deste contexto. Para Castro, Sabbag e Dantas (2017, p. 6), “É importante destacar que as transformações tecnológicas estão cada vez mais interferindo no modo de vida cotidiano e isso, precisa ser discutido e pensado de forma crítica para que as pessoas possam realmente acompanhar este ritmo”.

A Autoridade Nacional de Proteção de Dados (ANPD) é a entidade no responsável no Brasil, definida na legislação, com o escopo de elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade, e principalmente, fiscalizar e aplicar sanções em casos de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure contraditório, a ampla defesa e o direito de recurso. Também se encontra, dentre suas atribuições, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis (ANPD, 2020).

A proposta apresentada instrumentaliza ações de entidades reguladoras e de fiscalização, como a ANPD, que poderão adotar critérios objetivos para fiscalizar e auditar o compartilhamento de dados pessoais, bem como poderá contribuir no desenvolvimento de um padrão para registro das atividades de compartilhamento, aprimorando os direitos dos titulares de dados.

Diante de todo o exposto, o presente trabalho justifica-se como de relevância acadêmica e científica, na avaliação sobre a atual transparência oferecida aos titulares de dados no que tange a uma das atividades de tratamento de dados, o compartilhamento, e quais são os reais controles oferecidos aos cidadãos para rastrear fluxos de dados, podendo exercer seus direitos previstos nos novos regulamentos de proteção de dados pessoais. Apresenta-se, assim, uma proposição que realiza a experimentação científica da tecnologia *Blockchain*, e como ela pode contribuir com os processos de organização e recuperação de informações relativas ao tratamento de dados pessoais. Justifica-se igualmente pela contribuição social, considerando que ao expor a opacidade vivida pelo titular de dados pessoais quanto aos fluxos dos seus dados pessoais pós cessão, apresenta uma proposta de modelo para registros das transferências de dados, o que permitirá aos titulares a informação e o conhecimento de “onde andam seus dados”, por meio de registros que ficarão armazenados na *Blockchain*, em nítido aprimoramento da privacidade, permitindo-os o exercício dos direitos trazidos com os novos regulamentos de proteção de dados.

1.5 PROCEDIMENTOS METODOLÓGICOS

O presente estudo caracteriza-se como uma pesquisa descritiva e analítica, com base em análise documental e revisão de artigos sobre o tema, divididas em duas partes: **a primeira**, caracterizada pela revisão da legislação Brasileira e Europeia de proteção de dados e levantamento de melhores práticas relativas ao compartilhamento de dados, e **a segunda**, de característica exploratória, com a análise de cinco aplicações com presença no Brasil, para identificar se efetivamente cumprem as leis e práticas estudadas ou não, e a proposição de um modelo para organização das informações sobre compartilhamento de dados pessoais com apoio da tecnologia *Blockchain*.

Trata-se de uma pesquisa descritiva, com abordagem qualitativa, De modo a identificar quais os direitos trazidos pelos regulamentos e as boas práticas relativas ao compartilhamento de dados, o trabalho utiliza os métodos a seguir apresentados:

1ª. Etapa - Levantamento legislativo e melhores práticas sobre compartilhamento de dados. Levantamento e análise da Legislação Brasileira de Proteção de Dados (LGPD) e *General Data Protection Regulation* (GDPR). O critério adotado para a revisão destes dois textos é que a Lei Brasileira é a única sobre a temática no País e a Lei Europeia, considerada uma norma “global” e que vem embasando a construção das Leis de inúmeros países. Após o levantamento legislativo, realizou-se uma pesquisa para se identificar os “*guidelines*” e melhores práticas envolvendo compartilhamento de dados, que especificamente tratam da atividade. Os critérios para seleção dos guias foram a representatividade e reconhecimento das entidades como referências na área de proteção de dados, respectivamente, emitidos por autoridades de proteção de dados e entidades que tratam do tema compartilhamento. Do mesmo modo, foram selecionadas melhores práticas focadas em “compartilhamento de dados” de nível mínimo nacional (ou de instituições de atuação nacional), descartando-se guias de cidades, localidades ou províncias. Foram analisados os *guidelines* das seguintes entidades:

- a) *Data Protection Commission of Singapore – Guide to data Sharing* (PDPC, 2018);
- b) *Information Commissioner’s Office – Data Sharing code of practice* (ICO, 2019);
- c) *Information Commissioner’s Office – Data Sharing code of practice* (ICO, 2020a);
- d) *Template data sharing agreement and data processing agreement* (BMA, 2019);
- e) A ética para compartilhamento de dados: Um guia para melhores práticas e governança (ACCENTURE, 2016);
- f) *Commission Nationale de l’Informatique et des Libertés - Transmission des données à des partenaires à des fins de prospection électronique: quels sont les principes à respecter* (CNIL, 2018);
- g) *Trusted Data Sharing Frameworks* (PDPC, 2019).

2ª. Etapa - Identificação das previsões e práticas na legislação e *guidelines* estudados, incluindo nomenclatura que utilizam para o tratamento de dados pessoais. Classificação das disposições em comum envolvendo compartilhamento de dados pessoais previstos nos referidos guias e legislação, incluindo análise dos termos que

designam para a operação de compartilhamento de dados. Identificação de práticas reconhecidas como necessárias para o compartilhamento de dados pessoais. Do mesmo modo, para nortear o entendimento sobre as operações de tratamento de dados pessoais, os termos previstos na legislação analisada foram correlacionados com o Ciclo de Vida de Dados (SANT'ANA, 2016), de modo a permitir a identificação sobre as terminologias utilizadas para operações de compartilhamento de dados.

3ª. Etapa - Pesquisa exploratória envolvendo revisão de Políticas de Privacidade de Aplicações e solicitação de informação sobre transferência de dados. Avaliação das políticas de privacidade da:

1. Rede social *Facebook*;
2. Buscador *Google*;
3. Mensageiro *WhatsApp*;
4. Aplicativo *fitness STRAVA*;
5. Fabricante *Samsung* especificamente para *SMARTVs*.

A avaliação se deu com a leitura das políticas de privacidade das redes e, a partir da mesma análise, identificando-se informações sobre a existência de termos envolvendo compartilhamento de dados pessoais, interpretação de e como definem “transferência de dados”, identificação se possuem contato para solicitações referentes a informações sobre tratamento de dados pessoais, identificação se informam o nome dos processadores e terceiros com os quais compartilham dados pessoais, se descrevem os dados compartilhados e se apresentam registros das operações de compartilhamento de dados. Do mesmo modo, identificou-se se as plataformas detinham formulários para contato em relação a dados pessoais, tendo-se realizado contato com as plataformas para identificar se respondiam ou não com os registros das atividades de compartilhamento de dados. O critério de seleção das aplicações foi a popularidade dos mesmos no País, sendo *Facebook*, *WhatsApp* figurando na lista dos 10 (dez) aplicativos mais utilizados pelos brasileiros (AGÊNCIA BRASIL, 2020). Já o *Google*, o maior buscador do mundo. Outro critério foi o tratamento de dados sensíveis, muito comum em aplicativos *fitness*, como o *Strava*. Por fim, foi relacionada uma aplicação envolvendo IoT (*Internet of Things*), com a análise da política de privacidade para *SMARTTVS* da fabricante *Samsung*.

4ª. Etapa - Identificação e extração dos resultados das análises. A partir do disposto na legislação e direitos identificados, bem como nos itens identificados nos *guidelines*,

como boas práticas no compartilhamento de dados, avaliou-se a transparência dos aplicativos e serviços *online*, identificando se ao titular dos dados existe ou não a possibilidade de rastrear os fluxos de seus dados pessoais, a partir do momento em que são coletados.

5ª. Etapa - Levantamento bibliográfico sobre compartilhamento de dados, privacidade e *Blockchain*. O levantamento bibliográfico foi realizado em nível internacional e em fontes bibliográficas da área de Estudo, nomeadamente, nos repositórios do *GOOGLE SCHOLAR*. O período do levantamento bibliográfico (recorte temporal) foi de 2015 a outubro 2020. Igualmente foi pesquisada a Legislação Brasileira de Proteção de Dados (LGPD) e *General Data Protection Regulation* (GDPR). Os termos de pesquisas utilizados foram, **em inglês**, '*blockchain AND data protection*', '*blockchain AND privacy*', '*blockchain AND information science*', '*blockchain AND data sharing*', '*blockchain AND personal data*', '*blockchain AND GDPR*', tendo sido recuperados somente os textos que tratam da aplicação e sua relação com compartilhamento de dados pessoais/registro de atividades envolvendo dados pessoais. Foram descartados artigos que tratavam de áreas específicas como por exemplo, registros de compartilhamento de dados pessoais médicos/saúde, considerando que o escopo do trabalho foi buscar textos genéricos e não direcionados a uma área do conhecimento. Na sequência, os artigos foram identificados, analisados e selecionados seguindo os seguintes critérios: pertinência ao tema escolhido e proximidade com a temática do compartilhamento de dados; atualidade dos documentos; relação da tecnologia *Blockchain* com aspectos relativos à privacidade e proteção de dados, previsão dos conceitos envolvendo compartilhamento de dados pessoais nos textos e que apresentam proposta para organização e recuperação de informações sobre compartilhamento. Os textos foram lidos, fichados de modo a observar a base teórica necessária para se identificar o estado da técnica envolvendo o uso da *Blockchain* para a proteção de dados pessoais e privacidade e práticas para compartilhamento de dados pessoais. As práticas analisadas foram utilizadas para subsidiar a elaboração da pesquisa e para a proposição do modelo para rastreamento das atividades de compartilhamento de dados. Foram revisados 10 (dez) artigos internacionais, identificando-se dados como: se apresentam a *Blockchain* como solução ou não; se preveem a questão do compartilhamento de dados; se apresentam padrão de descrição ou não; se descrevem um método; e, a partir dos achados, foram identificadas as limitações dos artigos propostos.

6ª. Etapa - Sistematização da proposta de registro das atividades de transferência de dados. A partir da revisão das pesquisas envolvendo a privacidade, proteção de Dados e *Blockchain*, sistematizou-se um modelo conceitual para registro das atividades de transferência de dados pessoais, de uso a agentes de tratamento de dados.

7ª. Etapa - Elaboração da Redação para o Exame de Qualificação. Apresentação à banca examinadora, das considerações preliminares sobre o estudo proposto.

8ª. Etapa - Elaboração da redação final de pesquisa. Consolidados os exames e análises, iniciou-se a construção de um modelo para registros das atividades de compartilhamento de dados pessoais, foram elaboradas as considerações finais da pesquisa com o intuito de divulgação à comunidade científica dos resultados obtidos com o desenvolvimento do estudo em questão.

A pesquisa bibliográfica foi realizada, no escopo de embasar a fundamentação teórica da pesquisa, do mesmo modo, no escopo de identificar o atual estágio das pesquisas sobre a temática (GIL, 2010) de modo a apurar os direitos dos titulares dos dados previstos na legislação, melhores práticas de privacidade (compartilhamento de dados) previstos em guias/códigos de práticas de Autoridades de Proteção de Dados, e como a *Blockchain* pode ser usada para o registro de dados relativos às transferências entre agentes de tratamento.

Posteriormente, nas fases 4 e 5, foi realizada a denominada revisão sistematizada da literatura, com a análise e interpretação das pesquisas disponíveis e consideradas relevantes para o objeto da pesquisa (KITCHENHAM, 2004), sendo possível identificar possíveis carências de pesquisas no tema, sugerir novas pesquisas e obter conclusões sobre um fato. Neste sentido, buscou-se identificar na revisão executada se ao titular dos dados são assegurados os direitos previstos nos regulamentos e *guidelines*, especificamente no que diz respeito à proteção de dados pessoais.

1.6 ESTRUTURA DO TRABALHO

A primeira seção, **Introdução**, trata dos pressupostos iniciais e a contextualização da importância do respeito à privacidade nas operações de compartilhamento de dados

peçoais, mostra a definição do problema; o núcleo da pesquisa: tese, hipótese e proposição; os objetivos (geral e específicos), motivação e justificativa da pesquisa e os procedimentos metodológicos, incluindo a descrição da estrutura do trabalho.

As demais seções são apresentadas na seguinte sequência:

A seção 2, **Compartilhamento de dados pessoais, proteção de dados e direitos dos titulares**, apresenta a conceituação de dados pessoais, identifica a operação “compartilhamento de dados” e suas características, disciplina quem são os atores nas operações de tratamento de dados pessoais e realiza a análise dos regulamentos brasileiro e europeu, visando identificar quais os direitos dos titulares de dados pessoais, especificamente no que diz respeito ao compartilhamento de dados.

A seção 3, **Códigos de práticas e *guidelines* de proteção e compartilhamento de dados**, avalia igualmente o código de prática e *guidelines* de autoridades de proteção de dados da França, Reino Unido, Singapura, além de entidades que regulamentaram ou documentaram o tema compartilhamento ou transferência de dados, buscando identificar pontos em comum nas práticas de compartilhamento de dados e se tratam da *Blockchain* ou de descrição de registros.

Na seção 4, **Avaliação dos aspectos de compartilhamento de dados em aplicações**, é realizada a análise exploratória das políticas de privacidade de agentes de tratamento de dados pessoais, especificamente 5 (cinco) aplicações com funções distintas, de modo a identificar, a partir dos direitos e práticas evidenciadas na seção anterior, quais oferecem ao titular o direito de conhecer quem são os agentes com que compartilham os dados e quais os fluxos existentes.

A seção 5, **A *Blockchain*, privacidade e a proteção de dados pessoais**, realiza a revisão sistemática de pesquisas internacionais relativas à tecnologia *Blockchain* e privacidade de dados, buscando identificar o atual estágio das pesquisas e mecanismos que permitam utilizar a infraestrutura como livro de registros de operações de tratamento de dados pessoais, buscando identificar, igualmente, aportes teóricos para a organização dos dados de compartilhamento para a propositura de um modelo conceitual.

Na seção 6, **Uma proposta para o registro descentralizado das operações de transferência de dados com base na *Blockchain***, com base no aporte teórico e revisões realizadas, é apresentada uma proposta de modelo conceitual para registro das operações de compartilhamento de dados, estruturado por metadados e com base na *Blockchain*, possibilitado aos titulares de dados consciência dos fluxos realizados com seus dados e

com conseqüente aprimoramento da privacidade dos indivíduos, nas operações de tratamento de dados pessoais.

A seção 7, **Considerações finais**, apresenta, por fim, os problemas identificados, consolidação das análises dos artigos que tratam da *Blockchain* no registro de atividades e como uma proposta para rastreamento das atividades de compartilhamento de dados pessoais contribui para o exercício dos direitos de proteção de dados dos indivíduos por meio da organização de informação e registros adequados.

2 COMPARTILHAMENTO DE DADOS PESSOAIS, PROTEÇÃO DE DADOS E DIREITOS DOS TITULARES

2.1 DADOS PESSOAIS, ANONIMIZAÇÃO, PSEUDONIMIZAÇÃO E ATIVIDADES DE TRATAMENTO

Dados pessoais são considerados dados que dizem algo sobre uma pessoa física, identificada ou que se possa identificar por meio de referenciamentos, inferências, reversão de códigos, associações a outros dados, dentre outros. Dentre os dados, são os que dizem respeito a uma pessoa natural.

São, assim, informações relativas a uma pessoa, identificada ou identificável, com base em informações distintas que possam levar à sua identificação.

Exemplos de dados pessoais são:

- o nome e apelido;
- o endereço de uma residência;
- um endereço de correio eletrônico como: nome.apelido@empresa.com;
- o número de um cartão de identificação;
- dados de localização (por exemplo, a função de dados de localização num telemóvel);
- um endereço IP (protocolo de Internet);
- testemunhos de conexão (*cookies*);
- o identificador de publicidade do seu telefone;
- os dados detidos por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca (COMISSÃO EUROPEIA, 2020a).

Para se tratar de dados pessoais, tem-se que pensar na palavra “vínculo” com o indivíduo. Conforme Doneda (2011, p. 93):

A informação pessoal, aqui tratada, deve observar certos requisitos para sua caracterização. Determinada informação pode possuir um vínculo objetivo sobre uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação se refere a características ou ações dessa pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou domicílio ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, sobre como opiniões que manifesta e tantas outras.

Para o autor, estabelecer o vínculo subjetivo é dinâmica importante, pois isso exclui outras categorias de informações, que, conquanto ligadas às pessoas, não são informações pessoais, como por exemplo, a propriedade intelectual.

Pierre Catala (1983, p.20, apud DONEDA, 2011, p. 94), por sua vez, ao conceituar dados pessoais, estabelece que este se caracteriza:

Mesmo que a pessoa em questão não seja a “autora” da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade.

Dados pessoais podem estar armazenados em bancos de dados, estes, considerados um conjunto de informações organizadas conforme determinada lógica, sempre com o viés utilitarista, ou seja, onde busca-se o máximo proveito do conjunto de informações. Importante distinção deve ser feita entre dados e informações. Dados teriam uma conotação mais “primitiva”, algo como “pré-informação” e a informação, por sua vez, estaria relacionada a algo além, à representação contida no dado, chegando ao limiar da cognição (DONEDA, 2011, p. 94).

Não se deve confundir, no entanto, dado e informação com conhecimento, apesar de estarem relacionados. Enquanto dado é uma sequência de símbolos, quantificados e qualificáveis, puramente objetivo e sem depender do usuário, a informação é abstração informal, representando algo significativo para alguém. Já o conhecimento é informação mais valiosa, porque a ele fora atribuído contexto, significado, interpretação. Conhecimento não pode ser inserido no computador por meio de uma representação, pois senão foi reduzido à informação (SETZER, 1999, p.12).

Davenport e Prusak (1998, p.4) apresentam elementos distintos entre dados, informação e conhecimento, a seguir apresentados (**Quadro 1**).

Quadro 1: Dados, informação e conhecimento

Dados	Informação	Conhecimento
Simple observações sobre o estado do mundo:	Dados dotados de relevância e propósito:	Informação valiosa da mente humana. Inclui reflexão, síntese, contexto:
Facilmente estruturados	Requerida unidades de análise	De difícil estruturação;
Facilmente obtidos por máquinas;	Exige consenso em relação ao significado;	De difícil captura em máquinas;
Frequentemente quantificados;	Exige necessariamente a mediação humana	Frequentemente tácito;
Facilmente transferíveis;		De difícil transferência;

Fonte: elaborado pelo autor a partir de DAVENPORT; PRUSAK (1998, p. 4-6)

Esta pesquisa dedica-se ao estudo dos dados pessoais que, tratados ou compartilhados indevidamente, podem revelar-se em informações e em conhecimento, servindo de base para tomada de decisões que podem gerar danos e discriminação, sobretudo, com o crescimento das tecnologias digitais do processamento e armazenamento de dados. Considera-se “dado” como um pedaço da informação ou uma suposição ou premissa a partir do qual inferências podem ser tiradas e revelar outros dados sensíveis.

Como estabelece Stefano Rodotà (1973 apud DONEDA, 2011), a novidade introduzida pelos computadores é organizar a informação até então dispersa. Neste contexto, deve-se ter cuidado adicional com uma categoria especial de dados pessoais, os chamados dados pessoais sensíveis, que são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Com as tecnologias digitais é possível, atualmente, a criação de modelos e a partir de dados de compra de uma pessoa, por exemplo, atribuir uma probabilidade de uma patologia, estado de saúde, logo, revelando-se dados pessoais sensíveis com possível precisão.

Como referenciou Pedro Bastos Lobo Martins (2019), referindo-se ao “*Caso Target*”:

O “Caso Target” já é conhecido por muitos e citado em quase todo texto que trata de Big Data e proteção de dados. Para os que não conhecem, em resumo, o pai de uma adolescente entrou em uma das lojas Target, uma empresa de varejo norte-americana, e ficou furioso ao descobrir que a companhia estava oferecendo cupons de desconto em produtos de bebê para sua filha. A reviravolta se dá quando, depois de um tempo, o pai liga para o gerente da loja e pede desculpas porque havia descoberto que sua filha de fato estava grávida. Esse caso foi relatado no ano de 2012, quando o conhecimento das possibilidades de uso de “Big Data” não era tão disseminado quanto hoje.

Embora já seja um caso bastante conhecido, ele continua sendo útil para introduzir a temática de proteção de dados. Um ano antes, a Target havia desenvolvido um modelo que era capaz de atribuir uma nota a consumidores relativas à probabilidade daquela consumidora estar grávida a partir de seu histórico de compras. Com esse modelo era possível inferir não só a probabilidade de gravidez, mas, com uma boa precisão, quando o bebê iria nascer. Isso permitia que a empresa enviasse cupons de desconto em estágios específicos da gravidez.

Esse é um ótimo exemplo de como a partir do processamento de dados que à primeira vista parecem triviais é possível se chegar a informações sensíveis e relevantes sobre alguém através de inferências.

Como se verá, o parágrafo primeiro, art. 11 da Lei Geral de Proteção de dados (BRASIL, 2018), ao abordar dos dados pessoais sensíveis, estabelece que estes não poderão ser tratados com base no legítimo interesse, não apenas os dados espontaneamente cedidos, mas também aqueles decorrentes de inferência e que revelem informações sensíveis, que possam causar danos aos titulares (que o categorizem, o classifiquem, o avaliem, indisponibilizem um serviço, violem um direito). Já outros dados pessoais revelados a partir de inferências, em tese, poderiam ser tratados com base no legítimo interesse, desde que cientificado o indivíduo:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica. (BRASIL, 2018, p. 1).

Inferências são, conforme Wachter e Mittelstadt (2019, p.14):

Informações relacionadas a uma pessoa natural identificada ou identificável, criadas através de dedução ou raciocínio lógico [*reasoning*] ao invés da mera observação ou fornecimento pelo titular. (WACHTER; MITTELSTADT 2019, p. 14, tradução nossa).

Com efeito, exemplifica-se no quadro abaixo (**Quadro 2**) hipóteses onde a partir do fornecimento espontâneo de um dado ou informação, inferências podem revelar outros dados pessoais, estes, que podem ser considerados sensíveis ou não.

Quadro 2: Dados inferidos a partir de dados fornecidos

Informação	Inferência	Tipo de dado	Categoria	Tratamento com base no Legítimo interesse
Uma pessoa que fornece apenas seu nome para contratação de um plano de saúde	Facilmente identifica sua origem étnica	Etnia	Pessoal Sensível	Não
Sujeito que se cadastra em uma rede social e fornece nome e <i>e-mail</i> , e a rede coleta a marca do celular	Pessoa com boas condições financeiras	Informações financeira	Pessoal	Sim
<i>Likes</i> em redes sociais	Predição do gênero e raça,	Gênero, raça, opção religiosa ou política	Pessoal Sensível	Não

	opção religiosa ou política			
Cliente realiza compras em um <i>e-commerce</i>	Hábitos de compra	Preferência de produtos	Pessoal	Sim
Cliente que informa seu CPF em fidelidade em uma farmácia	Doenças ou tratamento	Dados de saúde	Pessoal Sensível	Não

Fonte: elaborado pelo autor

Em tal cenário, o tratamento de dados inferidos sensíveis não poderia se dar com base no legítimo interesse, mas dependeria do consentimento. Já os dados pessoais inferidos não sensíveis, desde que informados adequadamente ao titular, poderiam ser tratados.

Por outro lado, adverte Pedro Bastos Lobo Martins (2019), ao defender soluções que tirem o peso da decisão do sujeito e gerem mais transparência, sobre os riscos de se compreender o consentimento como hipótese mais protetiva ao titular quando, na verdade, a dificuldade em visualizar como seus dados serão obtidos pode tornar esta opção a mais danosa:

Embora a princípio pareça contraintuitivo, confiar no consentimento como ferramenta de proteção do titular leva a uma menor proteção legal (SCHERMER et al., 2014; LAZARO, MÉTAYER, 2015). Devido a enorme assimetria informacional entre controlador e titular (principalmente se tratando de inferências), no momento do consentimento o titular não tem como saber quais informações serão obtidas sobre ele, de forma que nenhuma escolha significativa e proteção efetiva seriam garantidas (MARTINS, 2019, não paginado).

Os dados pessoais ainda podem ser anonimizados. Dados pessoais que tenham sido dissociados de seu titular, de modo que não seja mais possível a associação, são considerados dados anonimizados e deixam de ser considerados dados pessoais (COMISSÃO EUROPÉIA, 2020a). A anonimização de dados pessoais não pode ser realizada de qualquer modo.

Uma armadilha específica é considerar os dados sob pseudônimo equivalentes a dados anonimizados. O ponto relativo à análise técnica explica que os dados sob pseudônimo não podem ser considerados informações anônimas, uma vez que continuam a permitir que um titular de dados seja distinguido e passível de ser ligado a diferentes conjuntos de dados (GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º, 2014, p. 11).

Outras armadilhas identificadas no Parecer Técnico 05/2014 (GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º, 2014, p. 11) sobre técnicas de anonimização são especificadas como:

- a) Entender que quando os dados são anonimizados privam-se as pessoas de todas as garantias. Tal premissa não é verdadeira considerando que outros atos legislativos podem ser aplicados a estes tipos de dados. A exemplo, o disposto no art. 5º, número 3, da Diretiva relativa à privacidade das comunicações eletrônicas, que impede o armazenamento e acesso a informações de qualquer tipo em equipamentos terminais sem o consentimento do assinante/utilizador, pois tal faz parte do princípio mais amplo da confidencialidade das comunicações;
- b) Não mensurar o impacto do tratamento de dados anonimizados para geração de perfis. A utilização de conjunto de dados anonimizados e divulgados para utilização de terceiros também pode ser passível de originar a perda de privacidade, onde o parecer recomenda que devam ser avaliadas as expectativas legítimas dos titulares dos dados relativamente ao tratamento posterior dos dados que lhes digam respeito, considerando-se inclusive que a esfera da vida privada de uma pessoa singular encontra-se protegida pelo artigo 8.º da CEDH e pelo artigo 7.º da Carta dos Direitos Fundamentais da União Europeia.

Anonimização é, assim, a quebra do vínculo entre os dados e seus respectivos titulares (DONEDA, 2006, p. 44). É recorrente, no entanto, a divulgação de estudos sobre processos de anonimização falíveis e, neste sentido, qualquer dado pessoal anonimizado possui risco inerente de se transformar em dados pessoais, sobretudo diante da agregação de pedaços de dados que podem identificar a imagem de um sujeito, até então anônimo. Por outro lado, se para esta identificação exige-se um esforço razoável, não se pode considerar os dados pessoais, mas anônimos diante de “filtro de razoabilidade” necessário, que consideraria critérios como estado da arte da tecnologia, custo, tempo de reversão de acordo com as tecnologias existentes, além de se considerar a capacidade de engenharia reversa de quem trata os referidos dados (BIONI, 2019, p. 23-25).

Considerar que dados anonimizados também gozam de proteção é muito importante, já que muitas empresas costumam “anonimizar” dados para compartilhar sem autorização dos titulares de dados pessoais, o que pode constituir riscos à privacidade, sobretudo diante da agregação e inferências.

Há ainda uma outra característica dos dados pessoais. Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reidentificar uma pessoa. Ao contrário dos dados anonimizados, os dados pessoais pseudonimizados são considerados dados pessoais, abrangidos pelas regras trazidas pelos regulamentos de proteção de dados.

Exemplo citado por Bioni (2019, p. 25) diz respeito a uma grande rede de lojas varejistas que usa sua base de dados de programa de fidelidade para melhorar sua distribuição logística, com a estruturação de uma nova base de dados, sem saber quem são os consumidores, mas apenas com dados sobre os produtos com mais entrada e saída de acordo com o perfil dos estabelecimentos.

Este cenário, aparentemente de anonimização é na verdade de pseudonimização, considerando que, ao segmentar a base de dados, o agente de tratamento mantém ainda dados pessoais e meios para transformar o dado aparentemente anonimizado em um dado pessoal.

Deve-se igualmente, avaliar a capacidade subjetiva de terceiros que ingressaram no fluxo de informação da empresa, sobretudo diante de questões envolvendo enriquecimento de dados de modo a viabilizar uma atividade de tratamento (BIONI, 2019, p. 27).

Neste sentido, elabora-se um quadro (**Quadro 3**) com as categorias de dados, comumente manipulados por agentes de tratamento:

Quadro 3: Dados, informação e conhecimento

Categoria	Descrição
Dados pessoais	Dados que dizem respeito a uma pessoa, identificada ou identificável
Dados pessoais pseudonimizados	Dados que foram dissociados do seu titular, ou aplicadas técnicas para ocultação de sua identidade, de forma reversível
Dados anonimizados	Dados que foram dissociados do seu titular, de forma irreversível. Não são considerados dados pessoais
Dados pessoais sensíveis	Categoria especial de dados pessoais cuja revelação pode prejudicar direitos e liberdades individuais, implicar em dano e discriminação. São exemplos de dados pessoais sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Presunção de potencial discriminatório.

Fonte: elaborado pelo autor

Os regulamentos *General Data Protection Regulation (GDPR)* e Lei Geral de Proteção de Dados (LGPD) surgem em 2018 no escopo de proteger especificamente dados pessoais. Os regulamentos fazem frente a um cenário onde a geração tecnológica tem como grande elemento catalizador das empresas de tecnologia da informação e comunicação, a violação e a comercialização de dados pessoais (BOFF; FORTES, 2014).

Os regulamentos protegem os dados pessoais em relação a diversas operações de tratamento.

As operações de tratamento estão previstas no art. 4º, números 2 e 6 da *General Data Protection Regulation* e incluem a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. Já a Lei Geral de Proteção de Dados estabelece como operações de tratamento, em seu artigo 5º, inciso X, as atividades de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

São estas questões, aliás, tratadas no Programa de Pós-Graduação em Ciência da Informação da UNESP, que tem como eixo norteador o estudo crítico de teorias, metodologias e práticas voltadas à informação e ao conhecimento, com especial ênfase nos processos de produção, organização, representação, gestão, mediação, apropriação, recuperação e uso da informação, em que as tecnologias de informação e comunicação ocupam importante papel para o desenvolvimento científico, tecnológico e social da sociedade.

Sant’Ana (2016) apresenta um conceito para o Ciclo de Vida dos Dados Pessoais, também no escopo de reduzir a assimetria informacional (AKERLOF, 1970) que, como identificado em sua pesquisa, é danosa para os indivíduos e pode ser mais prejudicial do que os ganhos advindos das tecnologias de tratamento de dados em larga escala. De fato, a assimetria informacional em relação às atividades de compartilhamento de dados é imensa, não se concebendo ao titular o direito de conhecer os fluxos dos seus dados. Para o autor, a assimetria informacional é sustentada pelas camadas de recursos tecnológicos para uso dos dados, que tendem a ser mais profundas e complexas. Neste sentido, um esforço é feito para caracterizar os momentos envolvendo o tratamento de dados, conceituados como “coleta”, “armazenamento”, “recuperação” e “descarte”. Para cada

um dos momentos ou fases, fatores e características são consideradas, sendo elencadas como “privacidade”, “integração”, “qualidade”, “direitos autorais”, “preservação”.

Identifica-se nesta pesquisa (**Quadro 4**) a correlação entre as atividades de tratamento de dados pessoais previstas na legislação europeia, legislação brasileira e as fases do Ciclo de Vida de Dados (SANT’ANA, 2016):

Quadro 4: Quadro comparativo das atividades de tratamento de dados pessoais e fases do Ciclo de Vida dos Dados

GDPR (Art. 4, 2 e 6)	LGPD (Art. 5, inc. X)	Ciclo de Vida dos dados
Recolha	Coleta	Coleta
Registro	Armazenamento, arquivamento	
Organização	Classificação	Recuperação
Estruturação	Produção	Recuperação
Conservação	Recepção	Armazenamento
Adaptação	Processamento	Recuperação
Alteração	Modificação	Recuperação
Recuperação	Extração	Recuperação
Consulta	Acesso	Recuperação
Utilização	Utilização	Recuperação
Divulgação por transmissão, difusão ou qualquer outra forma de disponibilização	Comunicação, transferência, difusão. Distribuição	Recuperação
Comparação	(sem equivalente)	Recuperação
Interconexão	Transmissão	Recuperação
Limitação	(sem equivalente)	Recuperação
Apagamento	Eliminação	Descarte
Destruição	(sem equivalente)	Descarte
(sem equivalente)	Avaliação ou controle da informação	(sem equivalente)
(sem equivalente)	Reprodução	Recuperação

Fonte: elaborado pelo autor

Como se pode constatar, existem diferenças entre as operações de tratamento que são tratadas nas legislações. Já o Ciclo de Vida dos Dados possui momentos genéricos que podem enquadrar inúmeras atividades de tratamento previstas nas Leis. Este cenário confuso entre as nomenclaturas envolvendo as operações de tratamento de dados pessoais pode ser prejudicial aos agentes de tratamento (Atores) envolvidos nas operações com dados pessoais, e diante de dúvidas, prejudicar direitos e a privacidade de titulares dos referidos dados.

Conforme identificado no **Quadro 1** (p. 37), a Legislação Europeia *General Data Protection Regulation* (GDPR) diverge com a Lei Geral de Proteção de Dados no que diz respeito à nomenclatura das atividades de tratamento de dados pessoais. Para o

compartilhamento de dados, escopo desta pesquisa, o que a Lei Europeia trata como “Divulgação por transmissão, difusão ou qualquer outra forma de disponibilização” a Lei Brasileira entende como “Comunicação, transferência, difusão” ou “Distribuição”. Ambas as atividades estariam inseridas no âmbito do Ciclo de Vida dos Dados (SANT’ANA, 2016), na fase de “Recuperação”.

O compartilhamento de dados pessoais, objeto desta pesquisa, é uma das operações previstas em ambos os regulamentos, tanto no Europeu, **“Divulgação por transmissão, difusão ou qualquer outra forma de disponibilização”**, como na legislação Brasileira, onde se pode identificar a **“Comunicação, transferência, difusão” e, também, a operação “Distribuição”**. O compartilhamento de dados pessoais no Ciclo de Vida dos Dados, enquadra-se no conceito de “Recuperação”, partindo do princípio já que se trata da fase em que se consideram esforços para que os dados sejam encontrados, acessados e interpretados, onde, igualmente, deve haver a preocupação com a privacidade dos dados e onde se avalia se o controlador tem ou não o direito de disponibilizar os referidos dados, e onde o apoio da Ciência da Informação se demonstra fundamental (SANT’ANA, 2016).

Como identificado, as diversas e complexas modalidades tecnológicas para compartilhamento de dados proveram uma opacidade na transparência que deveria existir para o titular de dados pessoais, sobre quem tem acesso a seus dados pessoais, o que fazem e por quanto tempo utilizam os referidos dados.

Constatou-se, tanto na legislação Brasileira, como na Europeia, princípios que asseguram ao titular dos dados o direito de conhecer as pessoas com quem se compartilham dados e quais os compartilhamentos realizados. Os princípios do livre acesso, qualidade, transparência na LGPD e os princípios da licitude, lealdade e transparência na GDPR asseguram estas garantias. A GDPR denomina majoritariamente as operações de compartilhamento como “transferência”, diversamente da LGPD, que trata a ação como “uso compartilhado de dados”. Como identificado na análise das Legislações, são previstos os direitos de acesso ao titular dos dados às operações de tratamento, incluindo os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados.

Embora previsto em lei como direito dos titulares de dados, ambas as normas não estabelecem como o titular pode exercer este direito. Do mesmo modo, o registro das operações de tratamento é previsto nos regulamentos sem, contudo, se estabelecer de que

forma estes dados serão armazenados, quando serão gerados, arquivados e como o titular terá acesso aos mesmos.

Apesar de a Lei Geral de Proteção de Dados nada estabelecer a respeito, a *General Data Protection Regulation* define em sua consideranda 63 o direito de o titular conhecer e ser informado sobre o tratamento de seus dados pessoais, sempre que possível facultando acesso a um sistema seguro por via eletrônica que possibilite ao titular acender diretamente a seus dados pessoais (GDPR, 2016).

É papel da Ciência da Informação projetar recursos que possam ser aplicados e desenvolvidos pela computação e que diminuam esta distância existente entre titulares e os fluxos de seus dados pessoais, permitindo aos mesmos, controle sobre suas informações pessoais. Identificado que o compartilhamento de dados pessoais integra as operações de tratamento de dados previstas nos regulamentos da Europa e do Brasil, avançou-se na pesquisa, igualmente, buscando identificar quais os atores envolvidos no processo de tratamento de dados pessoais e como os principais regulamentos tratam tais agentes, como são identificados, e quais os princípios de proteção de dados pessoais existentes.

2.2 ATORES ENVOLVIDOS NO TRATAMENTO DE DADOS PESSOAIS E A AUSÊNCIA DE TRANSPARÊNCIA

As operações de tratamento de dados pessoais são realizadas pelo que os regulamentos denominam agentes de tratamento, sendo estes os que realizam as referidas atividades de tratamento de dados pessoais.

Quem define as atividades e os meios pelos quais os dados serão tratados é denominado na Europa de “responsável pelo tratamento”. Uma empresa é considerada responsável pelo tratamento se decide por que e como os dados pessoais devem ser tratados, sendo que pode ocorrer que o responsável pelo tratamento atue de forma conjunta com outras empresas que tratam dados, sendo que estes devem estabelecer contratos que definam acordos para cumprimento da *General Data Protection Regulation* e conforme orientações da Comissão Europeia, estes acordos devem ser comunicados às pessoas cujos dados são objeto de tratamento (COMISSÃO EUROPÉIA, 2020b).

Do mesmo modo, a Legislação Europeia classifica aquele agente de tratamento que não tem condições de definir os meios e as finalidades do tratamento, mas age em nome de um responsável pelo tratamento.

Na Europa, este ator é denominado de “subcontratante”, que somente efetua o tratamento de dados pessoais sob instruções do responsável pelo tratamento e geralmente é um terceiro externo à empresa e em casos de grupos de empresas, uma empresa pode atuar como subcontratante de outra empresa. Assim, os deveres do subcontratante devem ser especificados por contrato, incluindo previsões sobre o que acontece com os dados uma vez finalizado o contrato, lembrando que um subcontratante só pode subcontratar as suas tarefas descritas ou contratadas pelo “responsável pelo tratamento” se tiver recebido autorização prévia e por escrito para esta atividade (COMISSÃO EUROPÉIA, 2020b).

A *General Data Protection Regulation*, do mesmo modo, estabelece na consideranda 74, que dispõe conceitos e explicações, a responsabilidade do responsável pelo tratamento em adotar e comprovar que as atividades de tratamento de dados estão em conformidade com a lei:

(74) Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares (GDPR, 2016, p. 1).

A legislação Europeia define as figuras do responsável pelo tratamento (aquele que determina as finalidades do tratamento) e subcontratante (organismo que trate dados pessoais por conta do responsável pelo tratamento):

Artigo 4.o
Definições

Para efeitos do presente regulamento, entende-se por:

7) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;

8) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes (GDPR, 2016, p. 1).

Destaca-se que o simples fato de existir uma cooperação entre vários sujeitos no tratamento de dados, como em uma cadeia, não significa que serão sempre corresponsáveis pelo tratamento, considerando que caso exista o intercâmbio de dados entre as partes, sem que ocorra uma partilha de finalidades ou meios em um conjunto

comum de operações, deverá ser considerado apenas uma transferência de dados entre responsáveis por tratamento distintos, como no exemplo tratado na documentação do Grupo de Trabalho do Artigo 29.º Sobre a Protecção de Dados:

Uma agência de viagens envia dados pessoais dos seus clientes às companhias aéreas e a uma cadeia de hotéis, a fim de fazer as reservas para um pacote de viagem. A companhia aérea e o hotel confirmam a disponibilidade dos lugares e quartos solicitados. A agência de viagens emite os documentos de viagem e os comprovativos da reserva para os seus clientes. Neste caso, a agência de viagens, a companhia aérea e o hotel serão três responsáveis distintos pelo tratamento, cada um deles sujeito a obrigações de protecção de dados em relação às suas próprias operações de tratamento de dados pessoais (GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECÇÃO DE DADOS, 2010, p. 24).

Uma rede social, a exemplo, é considerada pelo Grupo de Trabalho do Artigo 29.º Sobre a Protecção de Dados (2010) como responsável pelo tratamento, porém, os demais “utilizadores” da rede que carregam dados pessoais de terceiros também o são, desde que não sejam atividades abrangidas pela denominada isenção doméstica.

Já a pessoa física cujos dados são tratados é denominada pela legislação europeia como “titular de dados”, sendo a estes assegurado direitos de acompanhar “via sistema informatizado” as operações que são feitas com seus dados pessoais, conforme considerada 63 da GDPR (GDPR, 2016, p. 1):

Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software.

Embora previsto na legislação Europeia, a ausência de mecanismos e sistemas pelos quais os titulares de dados possam observar os fluxos com seus dados pessoais é notória, já que normalmente dependem de requerimentos a serem feitos aos controladores, que podem ou não serem atendidos. Não se tem um controle em tempo real destas atividades.

Ainda, a *General Data Protection Regulation* (GDPR) traz a figura do “terceiro”, o que define como sendo a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento

ou do subcontratante, estão autorizadas a tratar os dados pessoais (GDPR, 2016). O Parecer 01 (GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECÇÃO DE DADOS, 2010, p. 36) assim define terceiro:

Deste modo, «as pessoas que trabalham para outra organização, ainda que esta pertença ao mesmo grupo ou empresa-mãe, serão, em regra, consideradas terceiros», enquanto «os balcões de um banco que procedem ao tratamento das contas dos clientes sob a autoridade directa da sede não serão considerados terceiros.

Pode ser considerado “terceiro” o colaborador ou empregado, que tem acesso aos dados em decorrência do seu dever funcional.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) nomeia o responsável pelo tratamento como sendo “controlador” e o subcontratante, como o “operador”, definindo como “agentes de tratamento”, o controlador e o operador. Já a pessoa física dona dos dados pessoais é denominada de “titular” (BRASIL, 2018).

Art. 5º Para os fins desta Lei, considera-se:

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018, p. 1).

Ao controlador cabe o ônus de provar que o titular conferiu o consentimento para o tratamento de dados pessoais, quando a legislação assim exigir.

Tratando do Ciclo de Vida dos Dados, Sant’Ana (2016, p. 125) referencia os titulares de dados a “pessoas”, esclarecendo na dimensão “disseminação” dos dados que o acesso futuro aos dados deve ser considerado desde a fase de coleta de modo que uma maior encontrabilidade de acesso seja possível, exigindo-se que informações (atributos) que mesmo que não estejam ligados diretamente a necessidade atual sejam incluídas no planejamento da estrutura de obtenção, para que seja possível, por exemplo, elementos contextuais dos dados que possam favorecer sua localização e interpretação na fase de recuperação. Não se identifica uma menção expressa à figura do controlador de dados pessoais, embora o autor se refira a “detentor”, como aqueles que disponibilizam a informação a partir da fase de “recuperação” do Ciclo de Vida dos Dados, o que poderia se equiparar aos controladores, do mesmo modo se referindo a “usuário”, como a pessoa que tem acesso ou consome a informação de um CVD (**Quadro 5**):

Para a disseminação na fase de recuperação é necessário dotar os dados coletados e armazenados com elementos que permitam que os mesmos sejam encontrados por aqueles que irão utilizá-los, não bastando a simples possibilidade de acesso. São necessárias estratégias que permitam sua localização, não somente para acesso pelos próprios recursos de visualização de seus detentores, mas, também, por mecanismos automáticos que possam não só encontrá-los como ainda acessá-los em processos de coleta. Quando se trata de dados sensíveis, os usuários tendem a ter identificação forte e com direitos restritos de acesso, mas, mesmo assim, estes usuários precisam receber a informação de que aquele dado está disponível. Devem estar disponíveis, também, todas as informações sobre como usá-los, os aspectos semânticos envolvidos e, ainda, limitações de acesso, de tal forma que tudo isso possa ser identificado ainda no momento da localização, para facilitar a decisão sobre seu uso ou não (SANT'ANA, 2016, p. 134).

Quadro 5: Comparativo entre a nomenclatura dos atores e agentes de tratamento de dados pessoais

Definições	GDPR	LGPD	CVD (SANT'ANA, 2016)
Pessoa física a quem se referem os dados pessoais	Titular	Titular	Pessoa
Quem determina as finalidades do tratamento	Responsável pelo tratamento	Controlador	Detentor
Quem realiza o tratamento seguindo orientações do responsável pelo referido tratamento	Subcontratante	Operador	Usuários (embora o autor também se refira a estes como aqueles que consomem a informação)
Pessoa designada pelos agentes de tratamento como responsável por mediar as relações entre Autoridades e agentes de tratamento de dados	Encarregado de proteção de dados	Encarregado de proteção de dados	Sem correspondência
Qualquer outra pessoa que não seja titular, responsável pelo tratamento e operador	Terceiro	Sem correspondência	Sem correspondência

Fonte: elaborado pelo autor

Como identificado na pesquisa, apesar de ocorrer a divergência de nomenclatura em relação aos agentes de tratamento de dados pessoais, fica evidenciado que as legislações Europeia e Brasileira atribuem responsabilidades a ambos no que tange ao tratamento de dados. É identificado que as informações sobre compartilhamento de dados devem ser disponíveis aos titulares de dados, pois fazem parte de princípios e garantias previstas na legislação. Do mesmo modo, a pesquisa avaliou os direitos dos titulares de dados previstos em ambas as legislações (Europeia e Brasileira).

Sobre a responsabilidade dos agentes de tratamento de dados o Regulamento Europeu *General Data Protection Regulation* (GDPR, 2016), estabelece que quando dois

ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios deste tratamento, ambos são responsáveis conjuntamente.

Estabelece a norma em seu artigo 82 que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indenização do responsável pelo tratamento ou do subcontratante pelos danos sofridos, bem como que qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento (GDPR, 2016).

Por sua vez, a Lei Geral de Proteção de Dados Pessoais estabelece que o controlador e o operador que, em razão das atividades de tratamento, causarem danos de ordem patrimonial, moral, individual são obrigados a reparar o dano.

Operadores responderão solidariamente pelos danos causados pelo tratamento quando descumprirem a lei ou não tiverem seguido as instruções lícitas do controlador, momento em que será equiparado ao controlador. Do mesmo modo, respondem por danos decorrentes da violação da segurança de dados, o controlador ou o operador que causar dano ao deixar de adotar medidas de segurança, previstas no art. 46 da LGPD (BRASIL, 2018, não paginado):

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

Todos os controladores envolvidos no tratamento no qual decorreram os danos ao titular de dados respondem solidariamente. Os agentes de tratamento que participem de qualquer das fases do tratamento de dados obrigam-se a garantir a segurança da informação prevista em Lei. Por outro lado, nem sempre é claro, para o titular dos dados pessoais, quem são os demais controladores envolvidos, o que limita o exercício dos seus direitos.

Apresentados os atores que participam das operações de tratamento de dados, avança-se na apresentação dos princípios aplicáveis ao tratamento de dados pessoais.

2.3 PRINCÍPIOS DO TRATAMENTO DE DADOS E APLICAÇÃO AO COMPARTILHAMENTO DE DADOS PESSOAIS

É tendência nos ordenamentos jurídicos o tratamento autônomo da proteção de dados pessoais. A evolução legislativa sobre o tema avança ao longo das últimas quatro décadas. Doneda (2011) classifica o enfoque dado à proteção de dados pessoais durante a evolução legislativa, ao citar Viktor Mayer-Scönberger, apresentando quatro gerações de Leis, desde um enfoque mais técnico e restrito à vinculação da matéria a direitos fundamentais.

1ª Geração de Leis: Núcleo focado na concessão de autorização para criação de bancos de dados. Enfocavam o controle do uso das informações pelo Estado. Como exemplo, está a *Bundesdatenschutzgesetz*, Lei Federal da Alemanha de 1977 (DONEDA, 2011, p. 96). Neste momento a falta de conhecimento e familiaridade que as tecnologias geravam fez com que se lançassem princípios de proteção abstratos e amplos. Leis se tornaram rapidamente ultrapassadas.

2ª Geração de Leis: Surge no final da década de 1970, e tem como exemplo a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées*. Estas normas não estão centradas no fenômeno computacional, mas considera a privacidade e proteção de dados pessoais. Já se refletia na norma a insatisfação dos cidadãos em relação a seus dados tratados por terceiros, sem instrumentos de defesa.

3ª Geração de Leis: Surge na década de 80, com a percepção de que o fornecimento de dados pessoais por parte do cidadão se tornara indispensável e, com isso, o que era exceção se tornou a regra. Assim a terceira geração, manteve a proteção de dados pessoais centrada no cidadão, mas se preocupou com a garantia da liberdade do cidadão em fornecer ou não dados pessoais. (não apenas abranger tal liberdade). Esta geração estabelece meios de proteção caso a liberdade de decisão do cidadão fosse tolhida, assegurando a autodeterminação informativa.

4ª Geração de Leis: A quarta geração de Leis considera o pressuposto que não se pode tutelar os direitos dos titulares apenas com escolhas individuais, mas é necessário elevar o padrão coletivo de proteção. Geração marcada pelo fortalecimento da pessoa e das entidades de proteção de dados pessoais, redução do papel da posição individual na autodeterminação informativa. Nesta geração também se tem a disseminação do modelo de Autoridades Independentes e redução do “poder de barganha” com o indivíduo para autorização para tratamento de seus dados (DONEDA, 2011, p. 98).

Apesar da evolução das gerações de normas envolvendo proteção de dados pessoais, pode-se verificar o agrupamento de seus objetivos em princípios comuns, presentes desde a primeira até a quarta geração.

Danilo Doneda (2011, p. 99), ao tratar sobre o fracasso na tentativa de instituição do banco de dados nacional norte americano, *National Data Center*, elenca a força da discussão na área médica, no início da década de 1970, onde especialistas da *Secretary for Health, Education and Welfare* se reuniram e divulgaram em 1973 um estudo que concluiu pela necessidade de se estabelecer regras para o controle da própria informação. O documento previu meios de garantia ao cidadão a seus direitos, descritos como:

- Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.
- Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada.
- Deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento.
- Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito.
- Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados (DONEDA, 2011.p. 99).

Para o autor, tais regras procedimentais passaram a integrar inúmeras normativas de proteção de dados pessoais, passando-se a nominar “*Fair Information Principles*”. Elas foram maximizadas e expressas com um conjunto de princípios, sobretudo com a Convenção nº 108 do Conselho Europeu – Convenção para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais, denominada “Convenção de Strasbourg” (considerada principal marco de uma abordagem da matéria pela ótica dos direitos fundamentais, posteriormente previstos na Diretiva CE 95/46 e na Carta dos Direitos Fundamentais da União Europeia) e nos *Guidelines* da OCDE, logo no início da década de 80 (DONEDA, 2011, p. 100).

Segundo DONEDA (2011, p. 11) os princípios-chave que formam a espinha dorsal de inúmeras leis, tratados, convenções e acordos em termos de proteção de dados estão descritos no **Quadro 6**:

Quadro 6: Descrição dos princípios-chave de proteção de dados

Princípio	Descrição
Princípio da publicidade (ou da transparência)	A existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos
Princípio da exatidão	Os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade
Princípio da finalidade	Qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade)
Princípio do livre acesso	O indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos
Princípio da segurança física e lógica	Os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado

Fonte: elaborado pelo autor a partir da Tabela de Princípios (DONEDA, 2011, p. 100-101)

Como visto, embora não se tenha um princípio específico para a atividade de compartilhamento, aplicam-se a esta atividade os princípios da transparência, onde o titular deve ser informado sobre a formação de novos bancos de dados, bem como o princípio da finalidade, pelo qual restringe-se o compartilhamento de dados a terceiros além do permitido. Além do mais, o princípio do livre acesso pode assegurar que o titular conheça as operações de tratamento realizadas, inclusive as de compartilhamento. Nesta linha, o principal regulamento do Brasil e da Europa também estampam princípios para o tratamento de dados pessoais.

O tratamento de dados pessoais, tanto no Brasil, como na Europa, deve obedecer a boa-fé e princípios que informam e deverão ser observados pelos Agentes de tratamento de dados pessoais. Buscou-se identificar na Lei Geral de Proteção de Dados e *General*

Data Protection Regulation quais os princípios informadores e se estão relacionados a atividade envolvendo compartilhamento de dados pessoais.

A LGPD apresenta os princípios informadores no art. 6º (BRASIL, 2018, p. 1):

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (grifos do autor).

Do mesmo modo, a GDPR estabelece seus princípios para o tratamento de dados pessoais (GDPR, 2016, p. 1):

Artigo 5.o

Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («**licitude, lealdade e transparência**»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»). (grifos do autor).

A relevância desta pesquisa envolvendo os registros das atividades de compartilhamento de dados está relacionada com os princípios de proteção de dados pessoais previstos em ambos os regulamentos em análise. Na legislação brasileira, os princípios do **livre acesso, transparência e responsabilização e prestação de contas** asseguram ao titular de dados pessoais o acesso às informações sobre a forma de tratamento dos dados, bem como a obrigatoriedade de agentes de tratamento serem transparentes e prestarem contas sobre as operações de dados realizadas. Na legislação europeia, os princípios da **licitude, lealdade e transparência** também asseguram que o titular de dados terá direito de saber exatamente o que é feito com seus dados pessoais, o que inclui, logicamente, atividades de compartilhamento de dados pessoais.

Embora sejam os princípios garantias previstas nas legislações, a transparência prática nas operações de tratamento nem sempre são identificadas, sendo necessário a contribuição desta pesquisa para que os princípios previstos na norma sejam operacionalizados, com as informações necessárias para que se possa realmente obter transparência nas operações de tratamento de dados pessoais. Discutidos os princípios, analisa-se as premissas, ou as hipóteses legais em que agentes de tratamento podem manipular dados pessoais.

2.4 PREMISSAS PARA TRATAMENTO DE DADOS PESSOAIS

A atividade de tratamento de dados pessoais, incluindo o compartilhamento de dados, não poderá se dar de qualquer modo. Todos os agentes de tratamento ou “atores envolvidos no tratamento de dados pessoais” só estão habilitados a realizarem as operações de tratamento se, e somente se, estiverem amparados por umas das hipóteses legais que permitem o referido tratamento.

Pesquisou-se na legislação quais as premissas que habilitam o tratamento de dados pessoais. Na *General Data Protection Regulation*, o artigo 6º estabelece as hipóteses em que o tratamento de dados pessoais é permitido:

Artigo 6.o

Licitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

- a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
- c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
- d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
- f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança (GDPR, 2016, p. 1).

No Brasil, as premissas para tratamento de dados pessoais estão dispostas no artigo 7º. Da Lei Geral de Proteção de Dados Pessoais, que estabelece:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I - mediante o fornecimento de consentimento pelo titular;
- II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
- IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018, p. 1).

Como se constata, ambas as normas pesquisadas preveem premissas para tratamento de dados pessoais, que não necessariamente o consentimento do titular dos dados. No entanto, embora não haja a necessidade do consentimento em algumas hipóteses previstas na legislação, fato é que se outras operações forem realizadas ou os dados forem compartilhados para terceiros, o consentimento poderá ser necessário para estas operações específicas.

A GDPR estabelece que o consentimento pode ser dado para uma ou mais finalidades específicas e isso implica que o controlador deverá prever quando da coleta dos dados as finalidades que envolvam compartilhamento de dados a terceiros, inclusive referenciando-os. O que não significa dizer que o fato de informar em uma política de privacidade que o dado poderá ser compartilhado, que o agente de tratamento cumpriu com todas as garantias legais, pois como visto, o titular tem direito de conhecer as operações de tratamento realizadas com seus dados, incluindo as que compartilharam dados.

Assim, o controlador que obteve o consentimento e que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei (BRASIL, 2018). Comumente, as políticas e privacidade e proteção de dados pessoais solicitam o consentimento para um tratamento específico feito pelo controlador, prevendo que “poderá ocorrer” o compartilhamento de dados pessoais a terceiros sem, contudo, serem claras sobre quais os demais agentes que receberão, quando e como estas transferências serão ou foram realizadas. É esta dinâmica que explicita que bem sempre o consentimento é a opção mais protetiva ao titular de dados.

O compartilhamento de dados pode ser passivo, onde o agente controlador e que obteve os dados, disponibiliza interface de recuperação para que outros agentes obtenham a informação; ou pode ser ativo, onde o agente controlador remete, envia através de procedimento definido com terceiros, os *datasets* para que sejam processados por outros agentes. Em ambos os casos é essencial que ocorra a ciência do titular de dados, o que se avaliou nesta pesquisa. No entanto, proteger titulares de compartilhamentos de dados indevidos significa, primeiramente, compreender como vêm descrito e apresentado nas Legislações, o que se realizou neste trabalho.

2.5 O COMPARTILHAMENTO DE DADOS NAS LEGISLAÇÕES E OS DIREITOS DOS TITULARES DE DADOS

A *General Data Protection Regulation* e Lei Geral de Proteção de dados tratam de forma diferente a questão envolvendo o compartilhamento de dados pessoais. Enquanto na GDPR, esta atividade de tratamento é preponderantemente nominada de “transferência de dados”, na legislação brasileira, a expressão “uso compartilhado de dados” é a preponderante.

General Data Protection Regulation

- a) Transmissão de dados: 01
- b) Transferência de dados: 18
- c) Uso compartilhado de dados: 0

Lei Geral de Proteção de Dados

- a) Transmissão de dados: 0
- b) Transferência de dados: 1
- c) Uso compartilhado de dados: 14

Já a expressão “transferência” isoladamente considerada na GDPR é apresentada ou mencionada em 90 (noventa) oportunidades. A expressão “compartilhado” na LGPD é apresentada 19 (dezenove). A legislação Brasileira também equivale o termo “Uso compartilhado de dados” à atividade de “comunicação” de dados.

Avaliou-se, na sequência, se em ambas as legislações são previstos direitos dos titulares de dados pessoais e quais direitos são estes.

2.5.1 *General Data Protection Regulation*

A GDPR trata a questão envolvendo o compartilhamento de dados em seu art. 15, garantido aos titulares de dados:

Artigo 15.o

Direito de acesso do titular dos dados

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

- a) As finalidades do tratamento dos dados;
- b) As categorias dos dados pessoais em questão;
- c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais (GDPR, 2016, p. 1).

Percebe-se que conhecer os destinatários a quem os dados pessoais foram ou serão divulgados é um dos direitos dos titulares de dados previstos na legislação Europeia. Do mesmo modo, acerca do registro das atividades de tratamento, buscou-se identificar se a norma Europeia contempla esta disposição, tendo sido identificada a previsão de que os controladores de dados pessoais devem guardar um registro de todas as atividades de tratamento sobre sua responsabilidade (o que incluiria as atividades de compartilhamento de dados):

Artigo 30.o

Registos das atividades de tratamento

1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de **todas as atividades de tratamento sob a sua responsabilidade**. Desse registo constam todas seguintes informações:

- a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
- b) As finalidades do tratamento dos dados;
- c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;
- d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
- e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.o, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;
- f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
- g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.o, n.º 1. (GDPR, 2016, p. 1).

No que diz respeito aos registos das atividades de tratamento de dados pessoais, incluindo a atividade de compartilhamento de dados, identifica-se na *General Data Protection Regulation* a disposição da consideranda 82 (GDPR, 2016), que dispõe que a fim de comprovar a observância do regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser

obrigados a cooperar com a autoridade de controle e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento.

Do mesmo modo, o artigo 30 da legislação estabelece a obrigatoriedade da manutenção dos registos das atividades de compartilhamento de dados:

1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo constam todas seguintes informações:
 - d) | As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais (GDPR, 2016, p. 1).

Ainda, o mesmo artigo dispõe sobre a responsabilidade do subcontratante (no Brasil “operador” de dados pessoais) em manter não só o registo de todas as atividades que realizar em nome do responsável pelo tratamento, mas os dados do responsável pelo tratamento.

2. Cada subcontratante e, sendo caso disso, o representante deste, conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento, do qual constará:
 - a) | O nome e contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual o subcontratante atua, bem como, sendo caso disso do representante do responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados;
 - b) | As categorias de tratamentos de dados pessoais efetuados em nome de cada responsável pelo tratamento (GDPR, 2016, p. 1).

A norma Europeia também estabelece que os registos serão mantidos preferencialmente em formato eletrônico e deverão ser apresentados a Autoridade de controle se solicitados.

2.5.2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) prevê, dentre os direitos de titulares de dados pessoais, o de ter conhecimento sobre as empresas privadas ou públicas com as quais o controlador de dados pessoais compartilhou os dados:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (BRASIL, 2018, p. 1).

Por outro lado, a norma brasileira estabelece que o tema compartilhamento de dados poderá ser regulamentado pela Autoridade Nacional de Proteção de Dados. Assim, é possível que novas regulamentações sobre compartilhamento de dados sejam editadas: “Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais” (BRASIL, 2018, p. 1).

Do mesmo modo, o registro das operações de tratamento de dados pessoais é previsto na legislação. Embora não preveja expressamente a operação de compartilhamento de dados, a legislação estabelece que cabe aos agentes de tratamento (controlador e operador) manterem registros das operações de tratamento que realizarem: “Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse” (BRASIL, 2018, p. 1).

Ao deixar a cargo dos próprios agentes de tratamento a gestão das informações relativas ao compartilhamento de dados, evidentes são os riscos aos titulares, pois os dados não armazenados de forma transparente podem ser adulterados, modificados, excluídos ou modificados de modo a se omitir transferências não autorizadas.

2.5.3 Avaliação sobre os direitos trazidos envolvendo o compartilhamento de dados

Como identificado na análise das Legislações, a *General Data Protection Regulation* prevê os direitos de acesso ao titular dos dados às operações de tratamento, incluindo os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados.

No que diz respeito ao registro de atividades de tratamento, a legislação estabelece que “todas as atividades de tratamento” realizadas devem ser devidamente registradas, o que decorre também haver o dever de registrar as operações de compartilhamento de dados pessoais. Não se tem uma descrição sobre quais registros devem ser armazenados, o que também pode se caracterizar uma dificuldade de acesso aos titulares a tais operações e servir de base para omissões propositais.

Já a Lei Geral de Proteção de Dados Pessoais prevê o direito de o titular conhecer os agentes de tratamento com os quais o controlador realizou a transferência de dados, em seus artigos 9º e 18. Do mesmo modo, o registro das operações de tratamento de dados pessoais deve ser feito, com fundamento no art. 37 da norma, especialmente quando baseado no legítimo interesse.

Embora previsto em lei como direito dos titulares de dados, ambas as normas não estabelecem como o titular pode exercer este direito. Do mesmo modo, os registros das operações de tratamento são previstos no regulamento sem, contudo, se estabelecer de que forma estes dados serão armazenados, quando serão gerados, arquivados e como o titular terá acesso aos mesmos. Seriam apenas registros frios mantendo-se o nome de um destinatário de dados e tipos de dados que receberá, ou registros dinâmicos, gerados sempre que um compartilhamento for realizado?

Em tal ambiente, sem a organização de um padrão para registro de atividades de compartilhamento definido, ficará sobremaneira difícil ao titular dos dados efetivamente operacionalizar na prática os direitos trazidos nas referidas normas e conhecer quais dados são remetidos a terceiros e quando foram remetidos.

Analisou-se, na sequência, práticas de principais países em relação a proteção de dados de modo a buscar identificar se descrevem como deve ser o registro de compartilhamento de dados pessoais, em possível complementação aos regulamentos. A escolha dos países/entidades se deu diante de já terem publicado manuais ou conteúdo específicos em relação a compartilhamento de dados, a nível nacional.

3 CÓDIGOS DE PRÁTICAS E GUIDELINES DE PROTEÇÃO E COMPARTILHAMENTO DE DADOS

Como constatado, a revisão legislativa indica o dever dos agentes de tratamento em custodiar os registros das operações com dados pessoais. Por outro lado, não indicam quais as melhores práticas para o registro da operação de compartilhamento dos referidos dados. Investigou-se, assim, quais entidades já regulamentaram as leis de proteção de dados, por meio do estabelecimento dos Códigos de Práticas que tratam, especificamente, de compartilhamento de dados pessoais.

3.1 *Singapura Personal Data Protection Commission – Guide to Data Sharing*

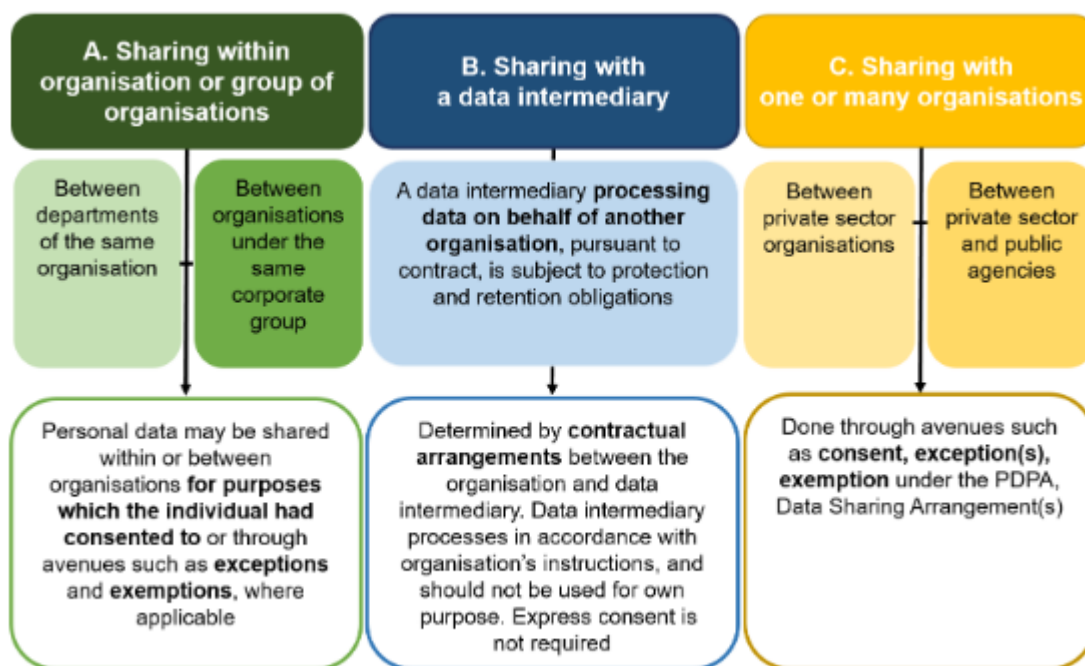
Em Singapura, a autoridade de proteção de dados *Personal Data Protection Commission (PDPC)* elaborou, em fevereiro de 2018, um guia de prática “*Guide to Data Sharing*” (PDPC, 2018). Regulamenta então o código *Data Protection Act* (SINGAPURA STATUS ONLINE, 2012), legislação local sobre o tema. O guia visa ajudar controladores de dados a realizarem a transferência de dados em conformidade com a legislação.

A boa prática apresenta 3 (três) formas existentes onde o compartilhamento de dados pode ocorrer:

- a) Compartilhamento dentro da organização: O compartilhamento só deve ocorrer para os propósitos que o titular tenha consentido ou com base nas exceções legais, quando aplicáveis;
- b) Compartilhamento com um intermediário: O compartilhamento de dados feito de um controlador para um processador de dados;
- c) Compartilhamento com outras organizações: O compartilhamento de dados feitos com outras organizações públicas e privadas (**Figura 1**).

Para o compartilhamento de dados internamente, deve-se garantir o consentimento do titular ou o respeito às bases legais para tratamento. Para o compartilhamento de dados com processadores, devem ser determinados arranjos contratuais para que o processador trate os dados de acordo com as organizações do controlador. Para compartilhamento de dados entre organizações, deverá ser feito com o consentimento ou com base nas exceções previstas em lei, bem como realizados os *Data Sharing Agreements*, que são contratos para que o compartilhamento possa acontecer.

Figura 1: Formas de compartilhamento de dados e obrigações



Fonte: PDPC (2018, p. 3)

A norma apresenta os fatores a serem considerados antes de compartilhamento de dados pessoais (PDPC, 2018, p. 6):

- Quais são os objetivos pretendidos do compartilhamento? Os objetivos são adequados às circunstâncias?
- Quais são os tipos de dados pessoais a serem compartilhados? Eles são relevantes para os fins pretendidos?
- Os dados anonimizados seriam suficientes no lugar dos dados pessoais para os fins pretendidos?
- O compartilhamento envolve a transferência de dados pessoais no exterior? É necessário consentir o compartilhamento? Existe uma exceção?
- É necessário notificar as pessoas sobre os objetivos do compartilhamento, mesmo que o consentimento não seja necessário?
- O compartilhamento envolve a transferência de dados pessoais para o exterior?

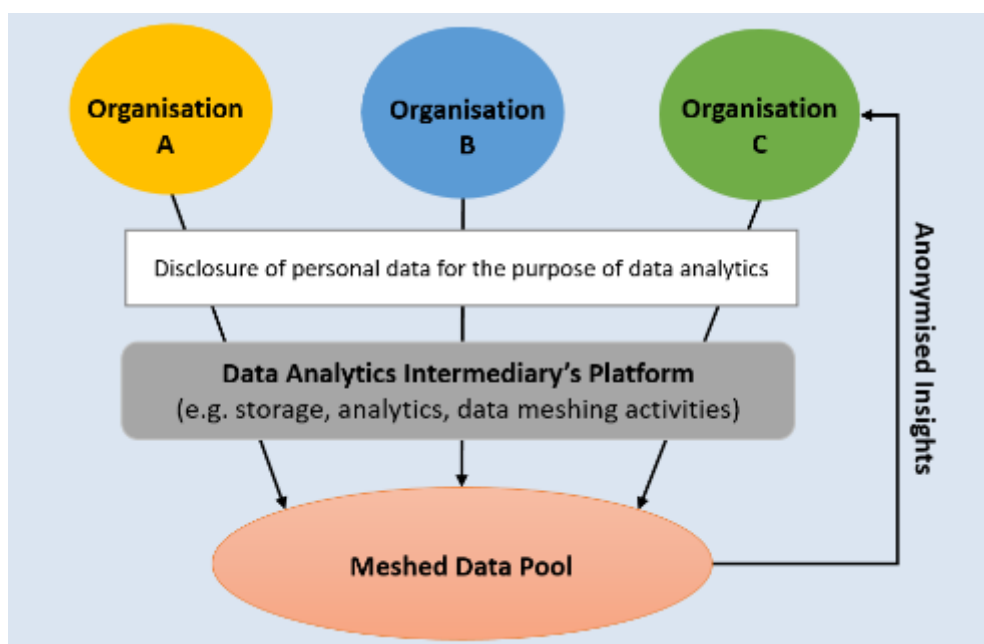
No que diz respeito ao compartilhamento de dados, o código de práticas da autoridade de proteção de dados da Singapura deixa claro que os controladores devem notificar os titulares de dados do interesse em compartilhar ou revelar seus dados antes de coletar os dados, obtendo o consentimento, caso não esteja amparado por uma exceção

legal. Se o controlador pretender compartilhar os referidos dados para um propósito diferente pelos quais obteve o consentimento, deverá informar o titular sobre esta atividade e obter o consentimento atualizado (PDPC, 2018).

Como se verifica, o Código preocupa-se em estabelecer como dever dos controladores de dados comunicar ao titular cada momento em que seus dados são compartilhados, quer para os propósitos especificados na coleta, quer não.

É possível, igualmente, que inúmeros controladores precisem compartilhar dados para uma empresa intermediária de *Data Analytics*. Nestes casos, é imprescindível que o consentimento esteja atualizado. Por outro lado, a partir dos dados recebidos, pode ser que a empresa de *Analytics* deseje compartilhar os “*Insights*” e resultados que apurou a partir dos dados recebidos pelos controladores. Nestes casos, caso haja um novo compartilhamento, o intermediário precisará de um novo consentimento, a menos que os dados estejam anonimizados (**Figura 2**).

Figura 2: Compartilhamento de dados para fins de análise (*analytics*)



Fonte: PDPC (2018, p. 3)

Não se esclarece como um “processador” fará contato com o titular de dados pessoais com a finalidade de informá-lo sobre a nova atividade de compartilhamento com os dados pessoais. O Código também descreve alguns métodos para obtenção eletrônica dos consentimentos considerados aceitos e válidos para norma local de proteção de dados, descrevendo-as como abordagens “dinâmicas de consentimento”:

Por exemplo, uma abordagem dinâmica para obter o consentimento pode ser implementada. Em vez de uma caixa de seleção única de conformidade, o consentimento pode ser uma opção contínua e gerenciada ativamente, com opções granulares oferecidas aos indivíduos em vários "pontos de contato". Esses processos podem ser aplicáveis, independentemente de a coleta ocorrer por meio de uma plataforma online ou offline pessoalmente. Isso permite que o mesmo conjunto de dados pessoais seja usado (ou reutilizado) com o conhecimento e consentimento dos indivíduos sempre que os objetivos de coletar, usar ou divulgar os dados pessoais forem alterados. Os indivíduos, por sua vez, terão mais controle sobre suas preferências de consentimento (ou seja, os indivíduos podem optar por dar ou retirar seu consentimento) e são mais propensos a fazer escolhas melhor informadas, pois seu consentimento está sendo obtido nas junções apropriadas. (PDPC, 2018, p. 11, tradução nossa).

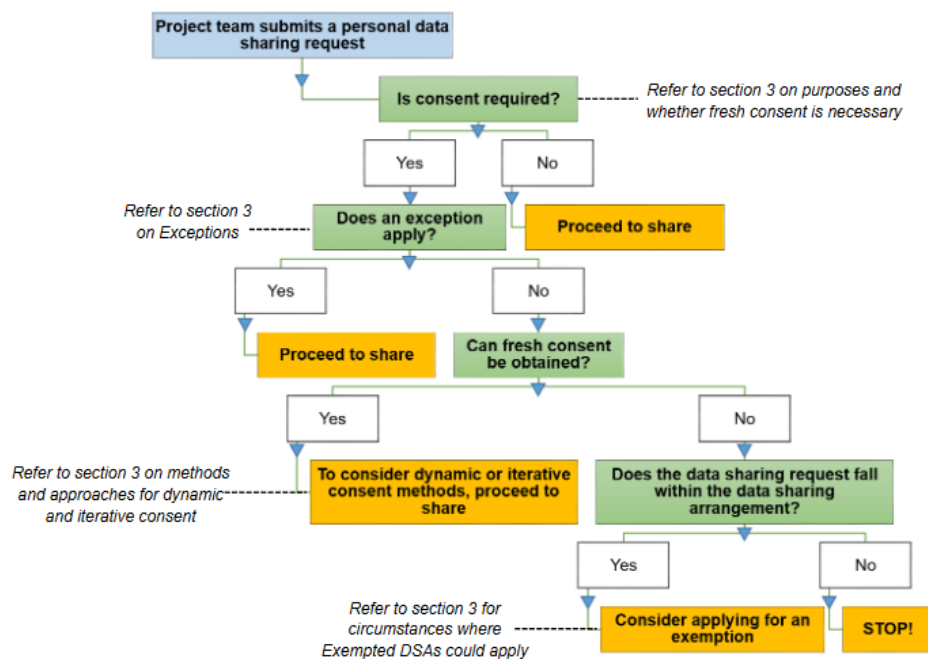
Ao tratar de abordagens dinâmicas, são apresentados ainda dois formatos de compartilhamento de dados, sendo elas:

- a) Notificações em tempo real: Notificações de *pop-up* enviadas a indivíduos imediatamente antes da coleta, uso ou divulgação de dados pessoais; tem o escopo de proporcionar meios interativos para se obter um novo consentimento;
- b) Painéis de proteção de dados: Os painéis de proteção de dados pessoais fornecem uma interface interativa para os indivíduos modificarem as preferências de proteção de dados em tempo real.

Uma organização pode fornecer um painel personalizado, permitindo que os indivíduos visualizem os dados pessoais que uma organização coletou sobre eles e como os dados pessoais estão sendo usados ou divulgados. Os indivíduos também podem facilmente entrar ou sair de qualquer finalidade ou qualquer outra coleta, uso ou divulgação de seus dados pessoais a qualquer momento (PDPC, 2018, p. 11, tradução nossa).

O *Personal Data Protection Commission (PDPC)* oferece um mapa mental sobre as atividades de tratamento de dados pessoais. O projeto de compartilhamento de dados pessoais surge em uma requisição de compartilhamento. Neste momento, avalia-se se o consentimento é necessário; se não for necessário o dado pode ser compartilhado. Se for necessário, avalia-se se existe alguma exceção legal; se existir, o dado pode ser compartilhado. Se o consentimento é necessário e não existe qualquer exceção legal que permita o compartilhamento, avalia-se a necessidade de atualização do consentimento. Se não houver a necessidade de atualização do consentimento, verifica-se se a ação se enquadra no acordo de compartilhamento. Se não se enquadrar em um acordo, deve-se parar imediatamente. Se existir, considere utilizar como uma exceção. Se a atualização do consentimento puder ser obtida, deve-se considerar os **métodos dinâmicos** ou interativos e proceder com o compartilhamento (PDPC, 2018) (**Figura 3**).

Figura 3: Workflow para requisição de compartilhamento de dados



Fonte: PDPC (2018, p. 22)

Pelo *workflow*, temos o seguinte procedimento:

- a) Uma área submete um requerimento de compartilhamento de dados;
- b) Avalia-se se o consentimento é requerido;
- c) Se o consentimento for requerido, avalia-se se existe alguma exceção;
- d) Se houver exceção, avança-se no fluxo do possível compartilhamento;
- e) Se não houver exceção e o consentimento for requerido, avalia-se se é possível obter o um consentimento atualizado;
- f) Se não for possível obter um novo consentimento, avalia-se se o pedido de compartilhamento de dados se enquadra em um acordo de compartilhamento;
- e) Se não se enquadra, o dado pessoal não pode ser compartilhado;
- f) Se enquadrar em um acordo de compartilhamento, pode-se considerar a aplicação de uma isenção.

3.2 Data Sharing: A code of practice

No Reino Unido, o *Information Commissioner's Office* (ICO, 2019) autoridade de proteção de dados, desenvolveu um guia denominado “*Data Sharing: a code of practice*”

(de 2011, mas em “*draft*” em 2019) O documento estabelece a necessidade da concepção e criação de um “*Data Sharing Agreement*”, documento que estabelece o propósito do compartilhamento de dados e o que acontece com os dados em cada fase, estabelece padrões e ajuda as partes na clareza em seus respectivos papéis, o que pode ajudar controladores e operadores a demonstrarem a conformidade com a legislação.

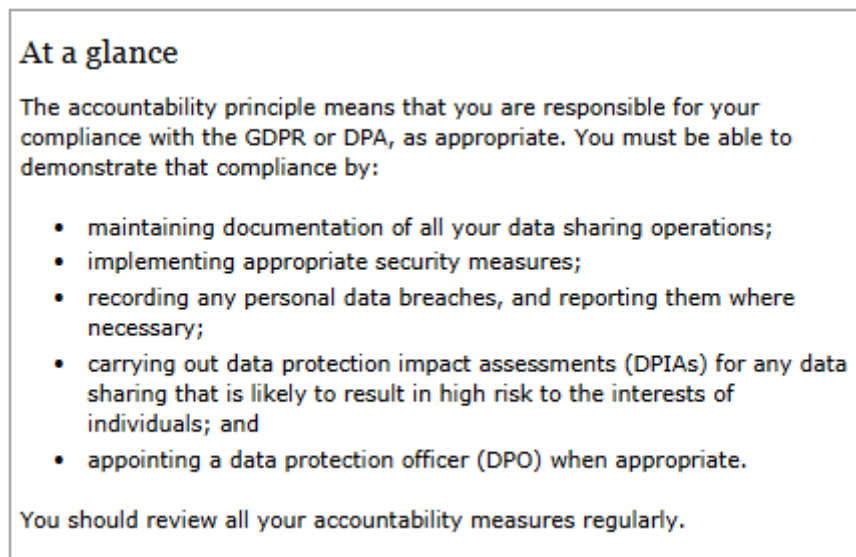
Dentre os itens que um “*Data Sharing Agreement*” deve conter, identificamos (ICO, 2019, p. 26):

- a) Qual o propósito do compartilhamento de dados?
- b) Quais empresas estão envolvidas no compartilhamento de dados?
- c) Estão sendo compartilhados dados para outros controladores?
- d) Quais itens na base de dados serão compartilhados?
- e) Qual a base legal utilizada para compartilhamento de dados?
- f) Existe alguma categoria especial de dados ou dados sensíveis?
- g) Previsão sobre os direitos dos indivíduos incluindo acesso aos registros?
- h) Quais informações de governança foram tomadas a respeito?
- i) Quais detalhes futuros devemos incluir?

No entanto, como se verifica, os *Data Sharing Agreements* não seriam eletrônicos, o que causa impedimentos ao titular dos dados em ter acesso a tais informações, o que dependeria sempre de requerimentos.

O Código de boas práticas estabelece igualmente princípios que devem estar presentes nas operações de compartilhamento de dados pessoais. Estes princípios anunciam o dever de manter a documentação de todas as operações de compartilhamento de dados (**Figura 4**):

Figura 4: Respeito ao princípio da prestação de contas no compartilhamento de dados



Fonte: (ICO, 2019, p. 32)

Como se identificou, o Código de Práticas regulamenta o artigo 30 da Legislação Europeia e cobra que algumas organizações mantenham registro das atividades de processamento (empresas grandes), incluindo as operações de compartilhamento de dados. O Código de Práticas estabelece, ao tratar da transparência nas operações de compartilhamento de dados, que é preciso garantir aos indivíduos o direito de conhecer o que acontece com seus dados, as organizações com as quais foram compartilhados os dados e devem ser informados sobre o propósito do compartilhamento, antes que ele ocorra:

Você deve garantir que as pessoas saibam o que está acontecendo com seus dados. Eles devem saber quais organizações estão compartilhando seus dados pessoais e quais têm acesso a essas informações, a menos que uma isenção ou exceção se aplique. Antes de compartilhar dados, você deve informar às pessoas o que você propõe fazer com seus dados pessoais de uma maneira que seja acessível e fácil de entender (ICO, 2019, p. 42, tradução nossa).

A norma também estabelece a necessidade da custódia de *logs* das atividades de processamento de dados, incluindo as transferências.

3.3 *Data Sharing code of practice* (2020)

Em dezembro de 2020 o *UK Information Commissioner's Office* (ICO) publicou seu novo código de compartilhamento de dados, atualizando o primeiro código publicado, de 2011. Dentre pontos cobertos pelo código, cita-se, conforme detalhado por Paul Greaves e Wim Nauwelaerts (2020):

a) Avaliação de impacto de proteção de dados: O código recomenda que sempre que o controlador de dados pessoais pretender compartilhar dados, deve ser realizada a avaliação de impacto de proteção de dados pessoais. Apesar do relatório de impacto, a proteção de dados só será requerida se o compartilhamento envolver alto risco aos titulares de dados. O código considera como uma medida indispensável para avaliação de riscos e mitigá-los;

b) Acordos de proteção de dados: O novo código do Reino Unido recomenda como boa prática os denominados *Data Sharing Agreements*, documentos que preveem o propósito do compartilhamento, procedimentos para *compliance* com direitos dos titulares e arranjos de governança de dados, como por exemplo, procedimentos para tratar de questões práticas, com estabelecimento de regras de exclusão ou retenção de dados compartilhados;

c) Definição das responsabilidades após compartilhamento de dados: A codificação estabelece que o controlador que recebe os dados pessoais será responsável pelos referidos dados. Deste modo, o controlador que recebe os dados deverá adotar medidas para garantir que os dados continuam protegidos. Define ainda pontos a serem observados pelos controladores;

d) Facilidade no exercício de direitos: O código do Reino Unido estabelece que devem existir procedimentos para que os titulares possam exercer seus direitos, e, em se tratando de requerimentos de titulares nas questões envolvendo compartilhamento de dados, prevê que seja criado um único ponto de contato com o titular, evitando que este tenha que realizar múltiplos requerimentos para controladores diversos que trataram ou tratam os dados.

O Código Britânico (ICO, 2020a), estabelece ainda que os controladores devem ter procedimentos claros para lidar com solicitações e requerimentos dos titulares de dados, de forma rápida e útil, além da necessidade de oferecer aos titulares informações sobre os dados compartilhados.

Um ponto inovador no Código Britânico é o Anexo B (ICO, 2020a, p. 77), que estabelece um padrão para requerimento de compartilhamento de dados pessoais, conforme apresentado no **Quadro 7**.

Quadro 7: ANEXO B - Modelo de Requerimento de Compartilhamento de Dados

Para uso pela organização que faz a solicitação de compartilhamento de dados.

Nome da organização

Nome e cargo da pessoa que solicita os dados

Se o solicitante não for o responsável pela proteção de dados (DPO) ou equivalente, ele foi consultado e suas opiniões foram consideradas?

Data do pedido

Descrição dos dados solicitados

Relação com o controlador de dados: Conjunta Separada

O solicitante tem um acordo de compartilhamento de dados em vigor? Sim Não

Objetivo do compartilhamento de dados.

O processamento envolve algum dado de categoria especial (ou processamento confidencial)?

Sim Não

Existem disposições específicas para retenção / exclusão de dados?

Há alguma circunstância no compartilhamento proposto que possa resultar em risco para os indivíduos?

Data (s) em que o fornecimento de dados é necessária

Fonte: ICO (2020b, p. 77-78, tradução nossa)

Assim, o código prevê um modelo de formulário (**Quadro 8**) para obter o consentimento dos indivíduos para o compartilhamento de dados pessoais, quando esta for a base legal, bem como um diagrama para mostrar como decidir se deseja compartilhar dados pessoais (GREAVES; NAUWELAERTS, 2020). Após a solicitação de compartilhamento de dados, um organismo que tomará a decisão sobre compartilhar os dados realizará uma avaliação, também com base no *template* proposto no Código de Boas práticas (ICO, 2020a, p. 79).

Quadro 8: Anexo B – Modelo de formulário de decisão sobre compartilhamento de dados

Para uso pela organização que irá tomar a decisão de compartilhar dados.

Nome da organização que recebe a solicitação para compartilhar dados

Nome da organização que solicita dados

Nome e cargo da pessoa que solicita os dados

Pedido de data recebido

Descrição dos dados solicitados

Relação do controlador de dados: Conjunta Separada

Teremos um acordo de compartilhamento de dados em vigor? Sim Não

Objetivo de compartilhar

Base legal para compartilhamento - indique qual Por que compartilhar é 'necessário'?

As condições adicionais são atendidas para dados de categoria especial ou compartilhamento de dados de ofensa criminal (quando aplicável)?

As disposições adicionais são atendidas no caso do compartilhamento de dados da Parte 3 DPA 2018?

Qual poder legal de compartilhamento se aplica (se relevante)?

Você já considerou um DPIA?

DPIA realizado e resultado (se aplicável)

As opiniões do DPO (ou equivalente) foram consideradas? (se DPIA não for feito) Existem disposições específicas para retenção / exclusão de dados?

Quais são as considerações de segurança?

Que medidas existem para cumprir os direitos de informação dos indivíduos?

Data (s) de compartilhamento solicitado (ou intervalos, se os dados forem compartilhados regularmente)

Decisão a pedido

Motivo (s) para compartilhar ou não compartilhar

Decisão tomada por (nome e cargo)

Assinado:

Data:

ICO (2020c, p. 79, tradução nossa)

Os campos previstos nos Anexos mostram dados sobre compartilhamentos que podem ser considerados para um sistema que registre tais atividades, além disso, sistemas computacionais e inteligência artificial poderão considerar as respostas e então avaliar se o dado pode ou não ser compartilhado. O código se distingue dos demais estudados pois vai além de prever transparência aos titulares, mas estabelece um formulário com informações mínimas que o titular deve ter, antes de uma atividade de compartilhamento ser iniciada.

Nas situações em que o consentimento não é necessário, no entanto, tais dados não deixam de ser relevantes, e podem ser armazenados, sobretudo os relativos à decisão de compartilhar, para que o titular possa consultá-los, valendo-se de seus direitos de ter acesso e informações sobre compartilhamento de seus dados pessoais.

A codificação também estabelece um anexo A (ICO, 2020d), onde apresenta um dever dos agentes de tratamento em documentarem a decisão sobre compartilhamento de dados, o que poderá ser solicitado por autoridades de proteção pelos titulares de dados.

O quadro abaixo (**Quadro 9**) estabelece as informações que precisam ser documentadas ou registradas pelos agentes de tratamento de dados, bem como o entendimento dos autores sobre a justificativa.

Quadro 9: Informações para serem registradas sobre o compartilhamento de dados pessoais

Informação registrada	Justificativa
Sua justificativa para compartilhar;	É necessário manter registros sobre a justificativa do compartilhamento de dados.
Que informações foram compartilhadas e com que finalidade;	Quais campos, registros, quantidade, natureza e categoria dos dados compartilhados.
Com quem foi compartilhado;	Dados dos agentes de tratamento que receberam os dados pessoais.

Quando e como foi compartilhado;	Qual a data, hora e de que forma os dados foram transferidos: Ex: uso de Apis, ftp, armazenamento/hospedagem, uso da plataforma, nuvem etc.
Se as informações foram compartilhadas com ou sem consentimento e como isso foi registrado;	Se o agente controlador obteve consentimento do titular ou não. Se obteve a prova do registro do consentimento.
A base legal para o processamento e quaisquer condições adicionais aplicáveis;	Qual a base legal utilizada para o tratamento dos dados pessoais.
Direitos dos indivíduos;	Quais os direitos que os titulares poderão exercer sobre a operação de compartilhamento.
Relatórios de avaliação do impacto da proteção de dados;	Manutenção de relatório que avaliou os riscos aos titulares de dados e quais medidas deveriam ser implementadas para reduzir, atenuar ou mitigar o risco.
Conformidade com qualquer conselho de DPO dado (quando aplicável);	Comprovação de que a transferência atendeu à conformidade.
Evidências das etapas que você executou para cumprir o GDPR e o DPA 2018, conforme apropriado;	Registros completos de todas as fases para conformidade com os regulamentos, antes da transferência dos dados
Onde você revisou e atualizou suas medidas de responsabilidade em intervalos apropriados.	Um plano demonstrando que as medidas são revisadas

Fonte: adaptado pelo autor de ICO (2020d)

3.4 Guidance note: *Template data sharing agreement and data processing agreement*

No Reino Unido, uma outra entidade que estabeleceu um código de compartilhamento é a *British Medical Association*, que publicou um guia de *templates* de acordo de compartilhamento de dados e acordo de processamento de dados. O regulamento aplicável à área médica define a necessidade dos acordos de processamento de dados. O texto, no entanto, não apresenta metodologia para consentimento automatizado/dinâmico ou para o registro das atividades de compartilhamento. No entanto, prevê que sistemas informatizados precisam estar configurados para compartilharem somente os campos necessários.

Para efetivar o compartilhamento de dados, será necessário saber exatamente quais campos de dados seus sistemas de TI precisam ser configurados para compartilhar com as outras Partes e exatamente quais campos de dados sua equipe pode esperar ver como recebidos da outra parte (BMA, 2019, p. 4, tradução nossa).

3.5 A ética do compartilhamento de dados: um guia para melhores práticas e governança

A consultoria *Accenture* (2016) publicou um guia sobre ética no compartilhamento de dados, boas práticas e governança. Como adverte, o compartilhamento ou a agregação de dados pode gerar inúmeros riscos de segurança, éticos e relativos à privacidade e requer atenção das empresas.

O aumento de recursos de computação em rede de baixo custo na nuvem pública permitiu que muitas organizações executassem análises avançadas sem investir em infraestrutura dispendiosa. Esses recursos permitem armazenar dados indefinidamente, movê-los imprevisivelmente e analisá-los repetidamente. O benefício de longo prazo dessas novas tecnologias reside na capacidade de compartilhar e mesclar dados dentro ou entre organizações, gerando um tremendo potencial econômico, estratégico e humanitário. Essas oportunidades, no entanto, devem ser consideradas juntamente com questões éticas. Dados os recursos humanos, financeiros e técnicos dedicados à coleta e gerenciamento de dados, existe uma obrigação ética de redefinir e compartilhar dados de uma maneira que maximize o bem que pode ser alcançado. Há também preocupações: por exemplo, focar apenas no benefício financeiro do compartilhamento de dados (com exclusão de tudo o mais) pode corroer a confiança dos parceiros ou dos que fornecem os dados. Isso poderia negar uma tremenda oportunidade para o bem. Com a devida consideração, no entanto, as oportunidades corporativas e éticas podem ser alcançadas (ACCENTURE, 2016, p. 4, tradução nossa).

O Código apresenta os desafios estruturais para a proteção do titular em relação ao compartilhamento dos seus dados. O consentimento, seja um consentimento informado em um contexto médico ou contratos de licença de usuário final para serviços de Internet, geralmente acontece como ponto de passagem obrigatório, no início da coleta de dados. Portanto, na medida em que os dados são cada vez mais utilizados fora do contexto inicial da coleta, existe uma lacuna problemática entre as ferramentas de análise de dados que dependem de compartilhamento e as ferramentas usadas para proteger os indivíduos dos danos que podem ser causados pelo compartilhamento (ACCENTURE, 2016).

O guia realiza a classificação de “camadas de compartilhamento de dados”, sendo elas (ACCENTURE, 2016, p. 11, tradução nossa):

- a) Intermediária: compartilhamento de dados entre parceiros, a mais complicada e menos discutida;
- b) Entidade: compartilhamento de dados interno, onde procedimentos internos podem ser adotados para preservar as garantias dos titulares de dados;
- c) Aberta: compartilhamento que já possui padrões e normas bem articulados.

Trata também das melhores práticas para a camada “intermediária”, considerada a mais problemática. Dentre as práticas, estão:

- a) Colaboração contínua entre os parceiros de compartilhamento de dados. O conjunto de dados não é estático, logo, os parceiros devem prestar contas uns aos outros pelo trabalho interpretativo sensível;
- b) Criação de contratos com o tratamento de todos os contratos e conjunto de dados como únicos, evitando-se uma padronização que não se aplica aos conjuntos de dados;
- c) Desenvolvimento de revisão ética entre os parceiros. Ambos os parceiros devem determinar antecipadamente como as questões éticas podem ser escaladas e resolvidas, tanto dentro de suas próprias organizações quanto entre elas;
- d) Os parceiros são mutuamente responsáveis pelos recursos interpretativos. Para o caso de uso de aprendizado de máquina e outros modos de análise de dados, há o dever de se enumerar as suposições;
- e) Identificar riscos potenciais do compartilhamento de dados;
- f) É preferível uma abordagem minimalista ao compartilhamento de dados. Neste ponto o código define claramente o direito do titular dos dados em avaliar o compartilhamento, antes do mesmo ocorrer:

Os titulares e destinatários de dados devem auditar cuidadosamente os conjuntos de dados para esses riscos antes de compartilhar todos ou alguns dos dados em consideração. Os termos do contrato relevante devem ser explícitos sobre o valor dos dados para cada organização participante” (ACCENTURE, 2016, p. 12, tradução nossa).

- g) Dados que parecem inócuos, em determinados momentos, podem ser prejudiciais quando combinados com outros dados, portanto, dados redirecionados requerem especial atenção. Os parceiros de compartilhamento de dados devem ter acordos explícitos sobre os parâmetros do direcionamento;
- h) Ao elaborar documentos, contratos ou políticas, ser sensível entre as tensões entre conformidade legal e a confiança com seus usuários. Os usuários merecem um documento que seja claramente compreensível e os ajude a se proteger.
- i) Quando a regulação e as leis não forem claras, é importante enfatizar o processo e a transparência. Neste sentido:

Particularmente à medida que o setor amadurece, a análise de dados geralmente opera em áreas cinzentas sem muito, se houver algum, precedente. Onde não existe um padrão industrial, processos de tomada de decisão transparentes e consistentes são a melhor proteção contra danos e uma maneira

de reforçar a confiança do público (ACCENTURE, 2016, p. 12, tradução nossa).

3.6 Código de Prática: Transmissão de dados aos parceiros para prospecção eletrônica: quais são os princípios a serem observados?

Na França, a Autoridade Nacional *Commission Nationale de l'Informatique et des Libertés* (CNIL) editou o Código “Transmissão de dados aos parceiros para prospecção eletrônica: quais os princípios a serem observados?”, escrito em francês, “*Transmission des données à des partenaires à des fins de prospection électronique: quels sont les principes à respecter?*”, onde estabelece melhores práticas para compartilhamento de dados pessoais. Muitas empresas que coletam dados diretamente de pessoas, *online* ou em papel, transferem estas informações para “parceiros de negócios” ou geralmente, para outras organizações. Esta transmissão deve respeitar uma série de condições.

O Código Francês estabelece uma série de princípios para os agentes de tratamento, sendo eles (CNIL, 2018):

- a) **A pessoa deve dar o consentimento antes de qualquer transmissão aos parceiros.** Na prática, não se identificou como a pessoa terá conhecimento do início de um compartilhamento e o Código não operacionaliza esta garantia;
- b) **A pessoa deve ser capaz de identificar os parceiros, destinatários dos dados, a partir do formulário em que os dados são coletados.** De outro lado, pode ser que nem sempre todos os parceiros estão previstos no formulário de coleta, o que demanda a necessidade de atualização do consentimento e transparência nas operações de compartilhamento;
- c) **A pessoa deve ser informada da evolução da lista de parceiros, em particular, da chegada de novos parceiros.** Esta comunicação, feita via envio de *e-mails* ou documentos é claramente prejudicial, razão pela qual é necessário o desenvolvimento de um modelo que organize a informação sobre novos agentes que terão acesso aos dados pessoais. O Código Francês estabelece claramente que estas informações podem ser disponibilizadas em dois níveis, possibilitando ao titular acompanhar o ciclo de vida dos dados com maior precisão e exercitar seus direitos com mais eficácia. As informações incluem o nome da empresa que transmitiu os dados ao parceiro, os direitos do titular dos dados, em particular, o direito de se opor ao compartilhamento:

Por exemplo, essas informações podem ser disponibilizadas em dois níveis, possibilitando acompanhar o ciclo de vida dos dados com mais precisão e exercitar seus direitos com mais eficácia:

- cada *e-mail* ou mensagem de prospecção recebida da empresa responsável pela coleta dos dados permite que você leia a lista atualizada de seus parceiros;
- cada novo parceiro que recebe os dados deve, ao se comunicar pela primeira vez com o cliente em potencial, informá-los, o mais tardar em um mês, do processamento que eles fazem dos dados (CNIL, 2018, p. 1, tradução nossa).

- d) **O consentimento coletado pela empresa que coleta dados em nome de parceiros é válido apenas para os parceiros.** Se a empresa está coletando dados em nome de um parceiro, não poderá compartilhar os referidos dados com seus próprios parceiros. **“Não existe transmissão de consentimento”** (CNIL, 2018, p. 1). Por outro lado, não identificamos a operacionalização prática desta boa prática. Como garantir que as empresas que coletam dados em nome de terceiros não estão, efetivamente, obtendo uma cópia dos referidos dados?
- e) **Os parceiros, por sua vez, quando receberem os dados, quando se comunicarem pela primeira vez com os titulares devem informar como exercer seus direitos, em particular objetar, bem como a fonte de onde provêm os dados utilizados.** Segundo o código francês de boas práticas, sempre que um parceiro receber os dados compartilhados, deveriam informar o titular dos dados, e neste momento possibilitando a este objetar o referido tratamento. Na pesquisa, identifica-se que na prática estas opções não acontecem para o titular de dados, dada a ausência de modelos de organização destes registros.

Como base no Código de Práticas da *Commission Nationale de l'Informatique et des Libertés* (CNIL, 2018), verifica-se que o titular deveria ser informado sempre antes do compartilhamento dos dados, devendo, igualmente, ser informando novamente pelo agente de tratamento que recebeu os referidos dados. Verifica-se que o código prevê a total ciência do titular dos dados sobre os fluxos dos compartilhamentos.

3.7 *Trusted Data Sharing Framework*

A *Personal Data Protection Commission Singapore* (PDPC) editou um *framework* denominado *Trusted Data Sharing Framework* (PDPC, 2019). O documento trata de pontos envolvendo a operacionalização do compartilhamento de dados pessoais, uma distinção em relação aos demais regulamentos que não trazem pontos “operacionais”.

Durante o processo de compartilhamento de dados, organizações devem procurar ser transparentes sobre como compartilham os dados e como eles serão utilizados. Provedores de dados e consumidores de dados devem ter acesso a como os dados foram processados e/ou manipulados para atender aos objetivos acordados. Deve ser estabelecido um contrato de compartilhamento de dados e como prática recomendada, as organizações devem preparar registros de auditoria e gerar registros para demonstrar responsabilidade e transparência na parceria de compartilhamento de dados. “Isso ajuda as organizações a garantir que os dados compartilhados foram gerenciados de forma correta” (PDPC, 2019, p. 50).

O *framework* enfatiza a necessidade de transparência nas operações de tratamento de dados pessoais, informando que fornecer informações aos titulares de dados é o caminho para obtenção da efetiva transparência, vejamos:

A transparência refere-se à abertura de todas as partes envolvidas no compartilhamento de dados para disponibilizar todas as informações necessárias para a entrega bem-sucedida da parceria de compartilhamento de dados. O princípio da transparência é contínuo e pode ser aplicado em qualquer parte da Estrutura, refletindo o contínuo relacionamento entre as organizações que estão compartilhando dados. A transparência e a confiança podem ser construídas através do compartilhamento de informações relevantes, como as relacionadas às práticas e políticas de negócios de cada organização, aos dados compartilhados e seus componentes e como os dados compartilhados serão usados. Por exemplo, é importante para os Consumidores de Dados declarar claramente, como eles usarão os dados fornecidos pelo provedor de dados. Isso pode ajudar os parceiros de compartilhamento de dados a criar confiança e estabelecer sua integridade no início de sua jornada de compartilhamento de dados (PDPC, 2019, p. 54, tradução nossa).

É também, para os casos em que a renovação do consentimento se faz necessária, reforçado os conceitos de “consentimento dinâmico” e “consentimento interativo”. O consentimento claro e específico obtido no início de um relacionamento com o titular de dados nem sempre pode atender todos os objetivos futuros, especialmente no cenário atual em que a mudança de modelos de negócios e novas tecnologias influenciam a maneira como as organizações coletam, usam ou divulgam dados pessoais e, neste contexto, se as organizações precisarem obter novo consentimento para novos propósitos de tempos em tempos, devem considerar a adoção de processos e métodos inovadores para cumprir os requisitos de consentimento exigidos por lei (PDPC, 2019, p. 72).

Uma abordagem dinâmica para obter consentimento pode ser implementada. Em vez de uma caixa de seleção de conformidade única, a aceitação de consentimento pode ser uma opção contínua e gerenciada ativamente, com opções granulares oferecidas aos indivíduos em vários "pontos de contato". Esses processos podem ser aplicáveis, independentemente de a coleta ocorrer por meio de uma plataforma *online* ou *offline* pessoalmente. Isso permite que

o mesmo conjunto de dados pessoais seja usado (ou reutilizado) com o conhecimento e consentimento dos indivíduos sempre que os objetivos de coletar, usar ou divulgar os dados pessoais forem alterados. Os indivíduos, por sua vez, terão mais controle sobre suas preferências de consentimento (ou seja, os indivíduos podem optar por dar ou retirar seu consentimento) e são mais propensos a fazer escolhas mais bem informadas, já que seu consentimento está sendo obtido em momentos apropriados. Riscos ou implicações para o indivíduo como resultado do compartilhamento de dados pessoais (por exemplo, se os dados pessoais contiverem informações confidenciais ou o compartilhamento puder afetar adversamente o indivíduo), o indivíduo deve ser informado sobre os possíveis riscos e implicações. Em geral, as organizações devem definir o padrão como "não compartilhar" e permitir que os indivíduos optem pelo compartilhamento de dados (PDPC, 2019, p. 72, tradução nossa).

O *Framework* também apresenta as tecnologias descentralizadas como poderosos instrumentos para instrumentalização da transparência previstas nas normas e regulamentos. Novas tecnologias permitiram estratégias e modelos de compartilhamento de dados mais sofisticados. As soluções “descentralizadas”, como a tecnologia de contabilidade distribuída, estão possibilitando novos modelos de troca de dados, mercados e serviços como *due diligence* de contrapartes, verificação de dados, segurança e certificação, contratação e governança (PDPC, 2019).

Assim, os mecanismos descentralizados são considerados para criação de uma “estrutura contratual”, para compartilhamento de dados.

Em um contexto multilateral ou descentralizado de compartilhamento de dados envolvendo Provedores de Serviços, eles podem criar confiança implementando uma estrutura legal para compartilhamento de dados que define os termos da licença de dados, incluindo o tipo/categoria de dados que podem ser extraídos, o uso permitido e a comercialização dos dados e as obrigações dos participantes (PDPC, 2019, p. 64, tradução nossa).

De forma inovadora para esta pesquisa, o *framework* em estudo cita a tecnologia *Blockchain*, como uma tecnologia descentralizada que pode auxiliar o trabalho de transparência dos fluxos de dados, o que fortalece a tese apresentada nesta pesquisa:

As organizações podem verificar se os *Data Service Providers* oferecem serviços que atenuam os riscos associados ao compartilhamento de dados com um público mais amplo, por exemplo, serviços de correspondência de dados que permitem a referência cruzada de banco de dados entre dois ou vários participantes para identificar clientes compartilhados sem fornecer acesso aos dados subjacentes e/ou sem transmitir dados pessoais. As organizações também podem verificar se as ofertas de serviços têm recursos que permitem controle sobre o fluxo de dados, como o uso de soluções de tecnologia como *blockchain* (PDPC, 2019, p. 27, tradução nossa).

A adoção de livros distribuídos é considerada como instrumento de transparência no *framework* de Singapura. Um livro distribuído é um consenso de dados digitais replicados, compartilhados e sincronizados espalhados por vários *sites* e usuários. É uma

alternativa à arquitetura típica do tipo contabilidade centralizada, em que uma autoridade central tem controle sobre as informações compartilhadas.

Especialmente nas situações em que todos os parceiros contribuem igualmente para as informações compartilhadas, uma arquitetura de contabilidade distribuída (registro distribuído) elimina uma autoridade central e depende da validação de cada parte (PDPC, 2019, p. 81).

A blockchain é um exemplo típico desse tipo de tecnologia. A natureza da blockchain garante que ela seja segura por design. Os parceiros de compartilhamento de dados podem, portanto, considerar as blockchains privadas como uma arquitetura de suporte para armazenar, processar, validar e autenticar informações. No entanto, as blockchains no momento não podem suportar grandes arquivos de dados e os parceiros de compartilhamento de dados que exigem transferências de grandes conjuntos de dados exigiriam outras formas de ledgers distribuídos. Um exemplo disso seria o local em que um grupo de bancos se reúne em uma parceria multilateral de compartilhamento de dados e contribui para um registro único com a validação de cada parte necessária para as transações (PDPC, 2019, p. 81, tradução nossa).

O *framework* trata a tecnologia *Blockchain* como de grande potencial para a finalidade de organização das informações sobre os fluxos de dados pessoais. De fato, quando combinada com computação segura, a tecnologia *blockchain* pode abrir um novo campo de possibilidades para o compartilhamento de dados, facilitando transações de dados confiáveis. O *framework* estabelece que os recursos elementares do *blockchain* – consenso distribuído, um livro resistente a violações que requer assinaturas digitais e contratos aplicáveis – permitem maior transparência e rastreabilidade e, portanto, promovem a confiança entre os parceiros de compartilhamento de dados (PDPC, 2019).

3.8 Avaliação regulamentos e dos códigos e boas práticas analisadas

Os regulamentos divergem quanto à nomenclatura adotada para os atores integrantes do contexto envolvendo proteção de dados e operações de tratamento. Identificou-se que ambos os regulamentos, Europeu e Brasileiro, descrevem como um direito de o titular de dados pessoais conhecer as pessoas públicas ou privadas com as quais os agentes de tratamento compartilharam dados pessoais. Em ambos os regulamentos o compartilhamento de dados está inserido no contexto de “operações de tratamento”, porém não há uma uniformidade de termos.

No que diz respeito ao registro das operações de tratamento, identifica-se que a Lei Geral de Proteção de Dados estabelece que tanto controlador quanto operador devem

manter o registro das operações de tratamento de dados pessoais que realizarem, porém, especialmente quando baseado no legítimo interesse.

Logo, a legislação Brasileira é mais branda, à medida que define que o registro das atividades de tratamento deverá se dar especialmente quando se tratar de um tratamento baseado no legítimo interesse.

Na legislação Europeia, igualmente, exige-se o registro das atividades de tratamento, tanto para operadores quanto para controladores de dados pessoais. No entanto, a legislação avança mais que a Brasileira, estabelecendo e descrevendo quais as informações devem constar destes registros de tratamento.

Os princípios que regulamentam a atividade de tratamento de dados pessoais, em ambos os regulamentos, preveem livre acesso e transparência dos agentes de tratamento de dados em relação ao titular, que devem ter o direito a consulta facilitada às informações sobre seus dados.

No entanto, não descrevem, operacionalizam ou indicam como agentes de tratamento podem dispor de sistemas informáticos de organização de dados para que possam satisfazer as necessidades de consultas por parte dos titulares de dados pessoais, motivo, aliás, que justifica a presente pesquisa, com a proposta de modelo que, se utilizados pelos agentes, proporcionará efetiva operacionalização prática dos direitos previstos nos regulamentos.

Como se verifica nos códigos de boas práticas analisados, todos estão preocupados com a transparência dos compartilhamentos de dados sem, contudo, estabelecerem protocolos ou padrões para que estes dados ou fluxos de compartilhamentos possam ser facilmente identificados pelo titular dos dados. No entanto, o *Trusted Data Sharing Framework* (PDPC, 2019, p. 47) avança, e estabelece os principais modos para compartilhamento de dados (**Figura 5**):

Figura 5: Meios comuns de compartilhamento de dados

	Wire	Removable Storage Media	Wi-Fi	Remote Access/ VPN	Object Storage URL / SFTP	API	Distributed Ledger
Continuous Access	✓		✓	✓	✓	✓	✓
High Volume of Data	✓			✓	✓	✓	
High Speed of Transfer	✓		✓	✓	✓	✓	
Highly Sensitive Data	✓					✓	✓
Affordability		✓	✓		✓	✓	
Secure by Design	✓						✓

Fonte: PDPC, 2019, p. 47

Identificou-se, ainda da análise dos códigos, que:

- Transparência:** A transparência nas operações de tratamento é item presente em todos os Códigos de boas práticas analisados nesta pesquisa. O Código Francês chega a afirmar que a pessoa deve ser capaz de identificar os parceiros, destinatários dos dados, a partir do formulário em que os dados são coletados e que a pessoa deve ser informada da evolução da lista de parceiros, em particular, da chegada de novos parceiros (CNIL, 2018);
- Acompanhamento do ciclo de vida e fluxos dos compartilhamentos:** O Código de Práticas da *Commission Nationale de l'Informatique et des Libertés* (CNIL, 2018) estabelece garantias ao titular de dados compartilhados em acompanhar os fluxos dos seus dados; Os códigos de Singapura, *Guide to Data Sharing* (PDPC, 2018) e *Trusted Data Sharing Framework* (PDPC, 2019), conquanto não trazem expressamente de acompanhamento de fluxos, apresentam previsões que permitem tal possibilidade como os “painéis de proteção de dados”;
- Contratos de tratamento de dados:** Os *Data Sharing Agreements* são previstos em todos os documentos investigados e são importantes instrumentos entre agentes de tratamento sobre as regras do compartilhamento;

- d) **Novos agentes de tratamento devem gerar comunicações ao titular:** Pode não ser possível identificar todos os agentes com os quais o controlador compartilhará os dados no momento da coleta, e, neste contexto, a pessoa deve ser informada da evolução da lista de parceiros, em particular, da chegada de novos parceiros (CNIL, 2018);
- e) **Painéis de proteção de dados:** Os painéis de proteção de dados são estabelecidos no *Guide to Data Sharing* (PDPC, 2018), como uma abordagem dinâmica onde os titulares podem visualizar como os dados vem sendo divulgados (PDPC, 2018, p. 11);
- f) **Consentimentos dinâmicos:** As abordagens dinâmicas de consentimento são tratadas no *Guide to Data Sharing* (PDPC, 2018) e no *Trusted Data Sharing Framework* (PDPC, 2019) como alternativas para revalidação do consentimento e para que o titular possa acompanhar os fluxos dos seus dados pessoais. Como verificado, o consentimento claro e específico, obtido no início de um relacionamento com o titular de dados, pode nem sempre ser capaz de atender aos propósitos futuros, sobretudo no cenário onde os modelos de negócios mudam e as novas tecnologias influenciam a forma como as organizações compartilham dados. E é neste cenário que os controladores podem considerar métodos inovadores, como abordagens dinâmicas, para obtenção do consentimento, com opções granulares em uma plataforma *online* ou *offline* (PDPC, 2019, p. 72);
- g) **Uso da Blockchain:** O *Trusted Data Sharing Framework* (PDPC, 2019) é o único Código que trata da *Blockchain* ou dos registros não centralizados para aumentar a transparência ao titular dos dados pessoais nas operações de compartilhamento. As soluções “descentralizadas”, como a tecnologia de contabilidade distribuída, estão possibilitando novos modelos de troca de dados, mercados e serviços como *due diligence de contrapartes*, verificação de dados, segurança e certificação, contratação e governança (PDPC, 2019);
- h) **Formulários modelos. Dados necessários para solicitação de compartilhamento de dados:** O guia *Data Sharing: a code of practice* (ICO, 2020d), contempla um anexo A, onde prevê um *checklist* para a tomada de decisão sobre compartilhamento de dados. Do mesmo modo, no anexo B, apresenta dois modelos de formulários, com informações necessárias para se solicitar o compartilhamento de dados pessoais e para a tomada de decisão sobre o compartilhamento.

Neste cenário, os resultados são apresentados no **Quadro 10**. Como se verifica nos itens analisados, nos principais códigos de práticas de compartilhamento de dados pessoais, conquanto transparência e contratos de compartilhamento de dados (**questões jurídicas**) estejam presentes em todos os documentos, procedimentos operacionais e técnicos para que o titular efetivamente possa conhecer o fluxo dos seus dados pessoais (**questões informacionais**) estão presentes apenas nos Códigos elaborados pela *Personal Data Protection Commission Singapore (2018 e 2019)*, o que expõe o objetivo da pesquisa em demonstrar que os direitos dos titulares estão inviabilizados diante da ausência de mecanismos informacionais e computacionais que os operacionalizem.

Quadro 10: Avaliação dos Códigos e Práticas de Compartilhamento de Dados

Código	Item avaliado/identificado	Trusted Data Sharing Framework (PDPC, 2019) - Singapura	Guide to Data Sharing" (PDPC, 2018) - Singapura	Transmissão de dados aos parceiros para prospecção eletrônica: quais os princípios a serem observados (CNIL, 2018) - França	Data Sharing: A code of practice (ICO, 2019) - Reino Unido	Data Sharing: A code of practice (ICO, 2020) - Reino Unido	Guidance note: Template data sharing agreement and data processing agreement (BMA, 2019)	Ética no compartilhamento de dados (ACCENTURE, 2016)
1	Transparência							
2	Contratos/acordos de tratamento de dados							
3	Acompanhamento do ciclo de vida e fluxos dos compartilhamentos							
4	Consentimentos, abordagens dinâmicos							
5	Novos agentes de tratamento devem gerar comunicações ao titular							
6	Painéis de proteção de dados							
7	Uso da Blockchain/estruturas descentralizadas							
8	Formulários modelos. Dados necessários para solicitação de compartilhamento de dados							
9	Padrões ou protocolos práticos sobre como dever ser registrado o compartilhamento							
10	Métodos técnicos de compartilhamento de dados							

Fonte: elaborado pelo autor

A partir da análise dos códigos de compartilhamento de dados identificados com a extração das premissas e itens avaliados, nesta fase da pesquisa, foram avaliadas 5 (cinco) aplicações de grande densidade de usuários, para se apurar como tratam a questão da transparência do compartilhamento dos dados pessoais.

4 AVALIAÇÃO DOS ASPECTOS COMPARTILHAMENTO DE DADOS EM APLICAÇÕES

Analisou-se os termos de uso/privacidade de 5 (cinco) aplicações, no escopo de identificar como tratam a questão do compartilhamento de dados pessoais e a transparência nos processos de compartilhamento de dados. As aplicações analisadas foram a rede social *Facebook*, o buscador *Google*, o mensageiro instantâneo *WhatsApp*, o aplicativo *Fitness Strava* e as *Smartvs Samsung*.

4.1 CRITÉRIOS PARA A ESCOLHA DAS APLICAÇÕES

Os critérios para seleção das aplicações foram identificados na metodologia da pesquisa. As aplicações analisadas estão enquadradas em segmentos distintos e são populares no mundo e no Brasil.

4.2 TERMOS DE USO DO *FACEBOOK*

Os termos de uso da rede social *Facebook* são acessíveis através de URL¹ (FACEBOOK, 2020). Como se identifica, a rede apresenta uma área central com diversos assuntos sobre Privacidade. Nomeia sua política como “Política de Dados”. A rede social também dispõe de uma página sobre a *General Data Protection Regulation*, porém esta página apenas traz descrição da legislação europeia.

Pesquisou-se nas políticas das aplicações por expressões “compartilha” e suas derivações na Política de Dados, sendo que foram identificadas 47 (quarenta e sete) ocorrências. A expressão transferência (com radical “*transfer*”) retorna 6 (seis) ocorrências na Política de Dados (FACEBOOK, 2020).

Buscou-se então identificar como as redes sociais tratam o compartilhamento de dados dos titulares. Identificou-se que a rede social *Facebook* estabelece que os dados pessoais podem ser compartilhados com aplicativos, caso o titular dê permissões para tanto, identificando inclusive os dados que são coletados. Do mesmo modo, quando o titular dos dados pessoais utiliza as redes sociais em outras aplicações, como aplicações oferecidas por um Sistema Operacional, este sistema operacional poderá ter acesso às informações:

¹ <https://www.facebook.com/privacy/explanation>

Aplicativos, sites e integrações de terceiros em nossos Produtos ou que usam nossos Produtos.

Quando você decide usar aplicativos, *sites* ou outros serviços de terceiros que utilizam ou estão integrados aos nossos Produtos, eles podem receber informações sobre o que você publica ou compartilha. Por exemplo, quando você joga um jogo com seus amigos do *Facebook* ou usa um botão Comentar ou Compartilhar no *Facebook* em um *site*, o desenvolvedor do jogo ou do *site* pode receber informações sobre suas atividades no jogo ou receber um comentário ou *link* que você compartilha por meio daquele *site* no *Facebook*. Além disso, quando você baixa ou usa esses serviços de terceiros, eles podem acessar seu perfil público no *Facebook* e qualquer informação que você compartilha com eles. Os aplicativos e *sites* que você usa podem receber sua lista de amigos do *Facebook*, se você optar por compartilhá-la com eles. No entanto, esses aplicativos e *sites* não poderão receber outras informações sobre seus amigos do *Facebook* ou seguidores do *Instagram*, embora seus amigos e seguidores possam optar por compartilhar essas informações. As informações coletadas por esses serviços de terceiros estão sujeitas aos termos e políticas próprios, e não a esta Política.

Os dispositivos e sistemas operacionais que fornecem versões nativas do *Facebook* e do *Instagram* (ou seja, nos quais não desenvolvemos nossos próprios aplicativos) terão acesso a todas as informações que você optar por compartilhar com eles, inclusive as informações que seus amigos compartilharam com você, de modo que possam fornecer nossa principal funcionalidade (FACEBOOK, 2020, p. 1).

Do mesmo modo, se estabelece a possibilidade de compartilhamento de dados com parceiros externos, parceiros que usam o serviço de análise, anunciantes, parceiros de mensuração, parceiros que oferecem bens e serviços em nossos produtos, fornecedores e provedores de serviços, pesquisadores e acadêmicos, aplicação da lei ou solicitações legais (FACEBOOK, 2020).

O *Facebook* em nenhum momento indica quais são estes parceiros, não fornece alternativas para que o titular de dados não consinta com estas operações de compartilhamento, indicando apenas ao usuário que revise suas configurações: “Saiba mais sobre como controlar as informações pessoais que você ou outras pessoas compartilham com parceiros externos nas Configurações do *Facebook* e do *Instagram*” (FACEBOOK, 2020, p. 1, grifo do autor).

Igualmente, a rede informa que transfere dados para parceiros e para processamento nos Estados Unidos, sem citar quais (**Figura 6**):

Figura 6: Como o Facebook transfere os dados para prestar serviços globais

Como operamos e transferimos dados como parte de nossos serviços globais?

Compartilhamos informações globalmente, tanto internamente nas Empresas do Facebook, quanto externamente com nossos parceiros e com aqueles com quem você se conecta e compartilha no mundo todo em conformidade com esta política. Suas informações podem, por exemplo, ser transferidas ou transmitidas para, ou armazenadas e processadas nos Estados Unidos ou outros países fora de onde você mora, para os fins descritos nesta política. Essas transferências de dados são necessárias para fornecer os serviços estipulados nos [Termos do Facebook](#) e nos [Termos do Instagram](#), bem como para operar globalmente e fornecer nossos Produtos a você. Utilizamos [cláusulas contratuais padrão](#), seguimos as [decisões de adequação](#) da Comissão Europeia em relação a determinados países, conforme aplicável, e obtemos seu consentimento para essas transferências de dados para os Estados Unidos e outros países.

Fonte: FACEBOOK (2020)

Buscou-se identificar os contatos pelos quais os titulares possuem para identificar quais os parceiros com quem o Facebook compartilha dados e como isto acontece. Foi realizado o contato, através do formulário disponível, que não apresenta a opção “Lista de processadores que recebem seus dados pessoais” (**Figura 7**):

Figura 7: Dados de contato com Facebook

Como entrar em contato com o Facebook em caso de dúvidas

Saiba mais sobre como a privacidade funciona [no Facebook](#) e no [Instagram](#). Se tiver dúvidas sobre esta política, você pode nos contatar conforme descrito abaixo. Podemos resolver conflitos que você tenha conosco relacionados às nossas práticas e políticas de privacidade por meio da TrustArc. Você pode entrar em contato com a TrustArc pelo [site](#) da organização.

Entrar em contato conosco

Você pode entrar em contato conosco [online](#) ou pelo correio em:

Facebook, Inc.
ATTN: Privacy Operations
1601 Willow Road
Menlo Park, CA 94025

Fonte: FACEBOOK (2020)

Identificou-se assim as opções disponíveis para contato, tendo-se solicitado informações sobre “como o *Facebook* compartilha as informações que coleta” (**Figura 8**):

Figura 8: Contato feito com a rede social *Facebook*

The screenshot shows the Facebook help page for data policy questions. The URL is <https://www.facebook.com/help/contact/861937627253138>. The page features the Facebook logo and a search bar with the text "Como podemos ajudar?". Below the search bar is the "Central de Ajuda" (Help Center) navigation menu, which includes links for account creation, friend requests, home page, messages, photos and videos, Watch videos, pages, groups, events, payments, marketplace, apps, and accessibility. The main content area is titled "Perguntas sobre a Política de Dados" (Questions about Data Policy) and contains a list of questions with radio buttons for selection. The selected question is "How does Facebook share the information it collects?". Below the questions is a form to provide contact information, including a name field (filled with "José Antonio Maurilio Milagre de Oliveira") and an email field (filled with "ja.milagre@gmail.com"). A blue "Enviar" (Send) button is located at the bottom right of the form. The footer of the page includes the Facebook logo, copyright information (Facebook © 2020), language selection (Português (Brasil)), and various links such as "Sobre", "Privacidade", "Carreiras", "Opções de anúncio", "Criar anúncio", "Criar Página", "Termos e Políticas", and "Cookies".

Fonte: FACEBOOK (2020)

A resposta não chegou até o Autor, tendo sido remetido formulário em 19/04/2020. Não foi identificado prazo para resposta. Como constatado, a rede social não apresenta o nome e dados dos parceiros com quem compartilha dados dos titulares. Também não é possível solicitar o registro das transferências de dados feitas. Igualmente, a rede social não apresenta uma descrição detalhada dos dados pessoais que são compartilhados em cada transferência.

4.3 POLÍTICA DE PRIVACIDADE DO *GOOGLE*

Analisou-se a Política de Privacidade do buscador de Internet *Google* disposta no *link*² (GOOGLE, 2020). O *Google* não dispõe de uma página específica para tratar da Lei Geral de Proteção de Dados ou da *General Data Protection Regulation*. O *Google* armazena o versionamento de suas políticas de privacidade, onde foi possível identificar o *Download* em formato PDF (*Portable Document Format*).

Não existe uma política de dados específica. Foram identificadas 30 (trinta) correspondências para expressões exatas ou derivações de “compartilha”. Já para transferência (com radical “*transfer*”), foram identificadas 5 (cinco) ocorrências.

A Política de privacidade do *Google* estabelece que o titular dos dados pode compartilhar dados que podem se tornar públicos a outras pessoas. Do mesmo modo esclarece quando o *Google* compartilha as informações: “Não compartilhamos informações pessoais com empresas, organizações ou indivíduos externos ao *Google*, exceto nos casos descritos abaixo” (GOOGLE, 2020, p. 1).

Traz o *Google* 4 (quatro) exceções à regra de que não compartilha informações pessoais com empresas, organizações ou indivíduos, a seguir descritas:

Com sua autorização

Compartilharemos informações pessoais fora do *Google* quando tivermos seu consentimento. Por exemplo, se você usar o *Google Home* para fazer uma reserva por meio de um serviço de reservas, pediremos sua autorização antes de compartilhar seu nome ou número de telefone com o restaurante. Solicitaremos seu consentimento explícito para compartilhar quaisquer informações pessoais sensíveis.

Com administradores de domínios

Se você estuda ou trabalha em uma organização que usa os serviços do *Google* (como o *G Suite*), o administrador do domínio e os revendedores que gerenciam a conta terão acesso à sua Conta do *Google*. É provável que eles possam:

- acessar e manter informações armazenadas na sua conta, como seu *e-mail*;
- visualizar estatísticas da sua conta, como quantos apps você instalou;
- alterar a senha da sua conta;
- suspender ou encerrar o acesso à sua conta;
- receber informações da sua conta para atender qualquer legislação, regulação, ordem judicial ou solicitação governamental aplicável;
- restringir sua capacidade de excluir ou editar informações ou configurações de privacidade.

Para processamento externo

Fornecemos informações pessoais às nossas afiliadas ou outras empresas, ou pessoas confiáveis para processar tais informações por nós, de acordo com nossas instruções e em conformidade com nossa Política de Privacidade e quaisquer outras medidas de segurança e de confidencialidade adequadas. Por exemplo, usamos provedores de serviços para nos ajudar no suporte ao cliente.

² <https://policies.google.com/privacy>

Por motivos legais

Compartilharemos informações pessoais fora do *Google* se acreditarmos, de boa-fé, que o acesso, o uso, a conservação ou a divulgação das informações sejam razoavelmente necessários para:

cumprir qualquer legislação, regulação, processo legal ou solicitação governamental aplicável. Compartilhamos informações sobre o número e o tipo de solicitações que recebemos dos governos em nosso *Transparency Report*;

cumprir Termos de Serviço aplicáveis, inclusive investigação de possíveis violações;

detectar, impedir ou lidar de alguma forma com fraudes, problemas técnicos ou de segurança;

proteger de prejuízos aos direitos, à propriedade ou à segurança do *Google*, dos nossos usuários ou do público, conforme solicitado ou permitido por lei. (GOOGLE, 2020, p. 1, grifo do autor).

Como se verifica, o consentimento dado pelo titular de dados pessoais legitima o *Google* às operações de tratamento. Do mesmo modo, quando existem administradores de domínios como em uma conta *Gsuite*, estes também poderão acessar as informações na conta *Google*, incluindo *e-mail*. Ainda, sem consentimento do titular, o *Google* deixa claro que fornece informações pessoais às afiliadas e outras empresas para processamento de informações. No entanto, não esclarece em nenhum momento quais são estas empresas.

Fornecemos informações pessoais às nossas afiliadas ou outras empresas ou pessoas confiáveis para processar tais informações por nós, de acordo com nossas instruções e em conformidade com nossa Política de Privacidade e quaisquer outras medidas de segurança e de confidencialidade adequadas. Por exemplo, usamos provedores de serviços para nos ajudar no suporte ao cliente (GOOGLE, 2020, p. 1).

Também poderá o *Google* fornecer as informações após uma ordem legal. A política do *Google* prevê igualmente a cessão de informações “anonimizadas” para parceiros, mas não esclarece o processo de anonimização.

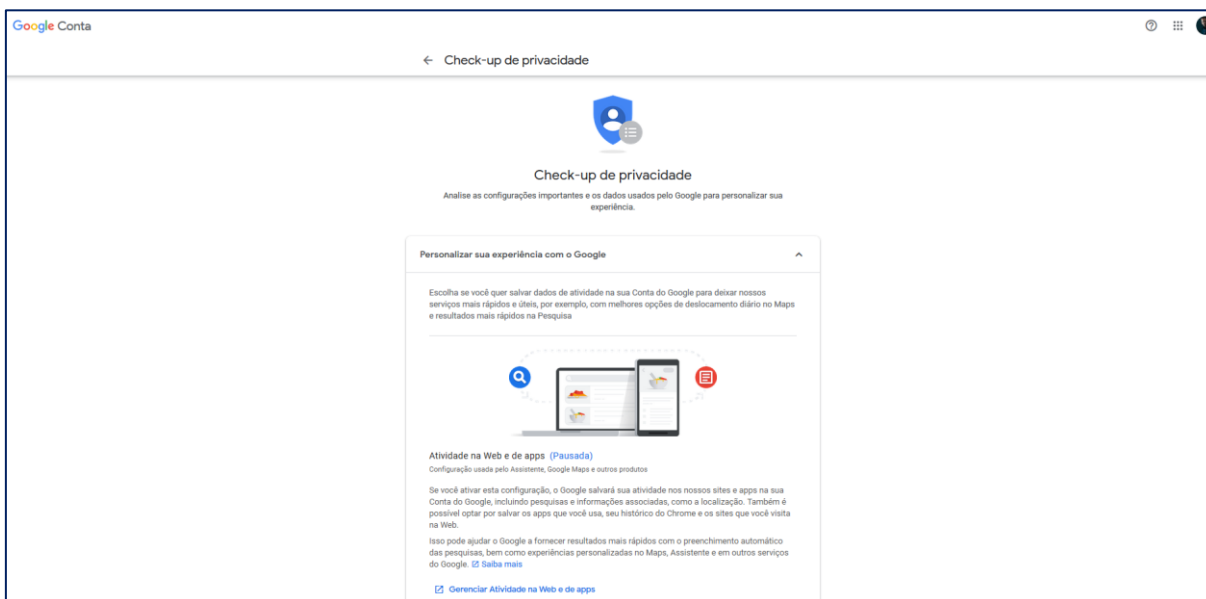
Podemos compartilhar informações de identificação não pessoal publicamente e com nossos parceiros – como editores, anunciantes, desenvolvedores ou detentores de direitos. Por exemplo, compartilhamos informações publicamente para mostrar tendências sobre o uso geral dos nossos serviços. Também permitimos que parceiros específicos colem informações do seu navegador ou dispositivo para fins de publicidade e medição usando os próprios *cookies* ou tecnologias semelhantes (GOOGLE, 2020, p. 1).

Não há transparência sobre como estes dados são compartilhados e quais são os parceiros. Do mesmo modo, a rede social não apresenta uma descrição detalhada dos dados pessoais que são compartilhados em cada transferência. Dentre as tecnologias usadas para coleta de dados estão *cookies*, *tags de pixel*, armazenamento local como

armazenamento do navegador da *Web* ou *caches* de dados de aplicativos, bancos de dados e registros do servidor. (GOOGLE, 2020).

A ferramenta permite ao usuário alguns controles sobre o que é coletado, como o *checkup* de privacidade (**Figura 9**), acessível pelo *link*³: (GOOGLE, 2020). No entanto, não existem controles para se evitar ou visualizar os fluxos de compartilhamento de dados:

Figura 9: Ferramenta *Checkup* de Privacidade



Fonte: GOOGLE (2020)

É possível, igualmente, verificar todas as atividades realizadas pelo titular no *Google* em *Minha Atividade*⁴: (**Figura 10**). Na própria Política de Privacidade do *Google* é possível exportar e excluir informações.

³ https://myaccount.google.com/privacycheckup?utm_source=pp&hl=pt_BR&pli=1

⁴ https://myactivity.google.com/myactivity?utm_source=pp&hl=pt_BR

Figura 10: Exportação e Exclusão de Informações na plataforma Google

Exportar, remover e excluir informações

Você pode exportar uma cópia do conteúdo da Conta do Google se quiser fazer backup ou usá-lo com um serviço fora do Google.

 [Exportar seus dados](#)

Você também pode [solicitar a remoção de conteúdo](#) de serviços específicos do Google com base na legislação aplicável.

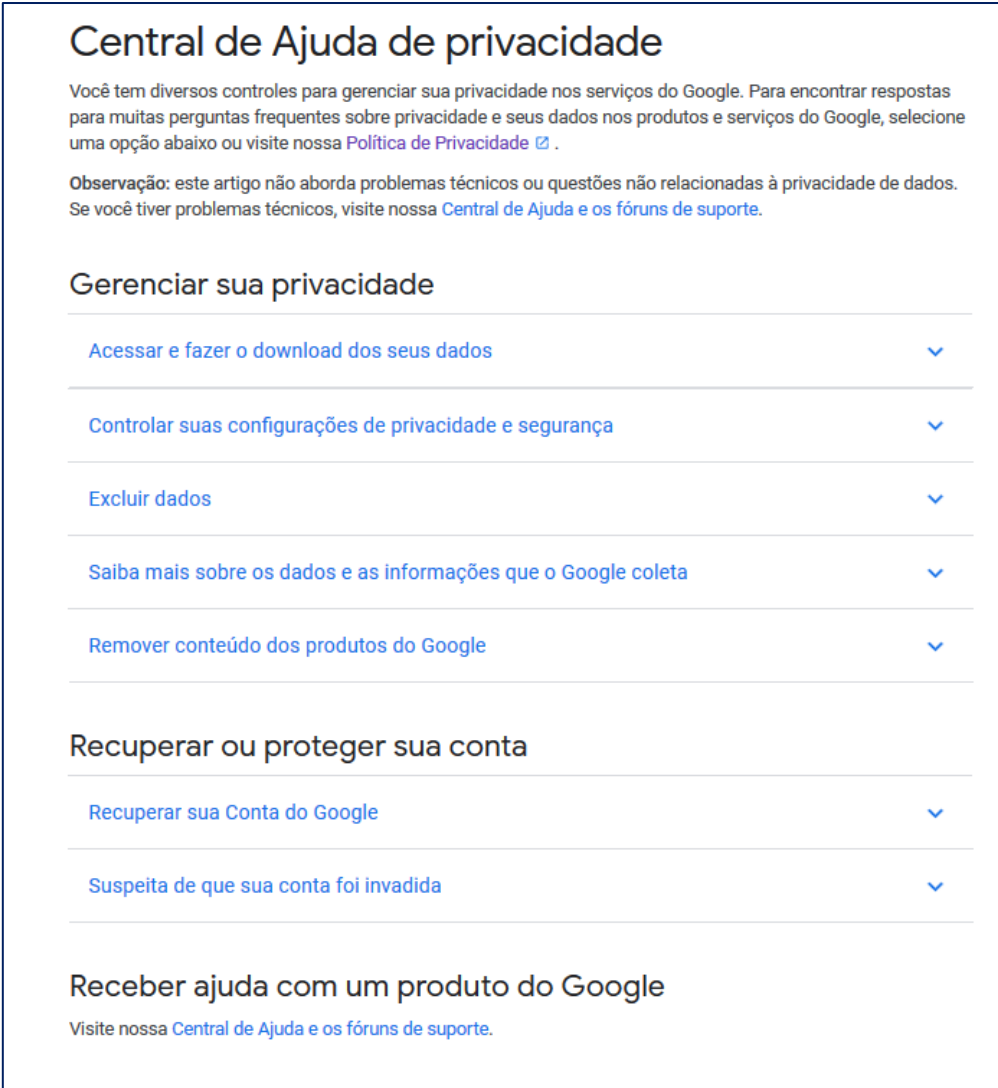
Para excluir suas informações, você pode:

- excluir seu conteúdo de [serviços específicos do Google](#);
- pesquisar e excluir itens específicos da conta usando [Minha atividade](#);
- [excluir produtos específicos do Google](#), incluindo as informações associadas a esses produtos;
- [excluir toda a sua Conta do Google](#).

 [Excluir suas informações](#)

Fonte: GOOGLE (2020)

A política não apresenta um contato físico, nem indicações de um encarregado de proteção de dados pessoais (*Data Protection Officer*). Ao se acessar o formulário de contato (**Figura 11**), verifica-se que não existe opção para que o titular possa conhecer com quais empresas realizou-se o compartilhamento de dados:

Figura 11: Opções que o titular de dados tem para obter informações sobre o *Google*

Central de Ajuda de privacidade

Você tem diversos controles para gerenciar sua privacidade nos serviços do Google. Para encontrar respostas para muitas perguntas frequentes sobre privacidade e seus dados nos produtos e serviços do Google, selecione uma opção abaixo ou visite nossa [Política de Privacidade](#) .

Observação: este artigo não aborda problemas técnicos ou questões não relacionadas à privacidade de dados. Se você tiver problemas técnicos, visite nossa [Central de Ajuda e os fóruns de suporte](#).

Gerenciar sua privacidade

- [Acessar e fazer o download dos seus dados](#) ▾
- [Controlar suas configurações de privacidade e segurança](#) ▾
- [Excluir dados](#) ▾
- [Saiba mais sobre os dados e as informações que o Google coleta](#) ▾
- [Remover conteúdo dos produtos do Google](#) ▾

Recuperar ou proteger sua conta

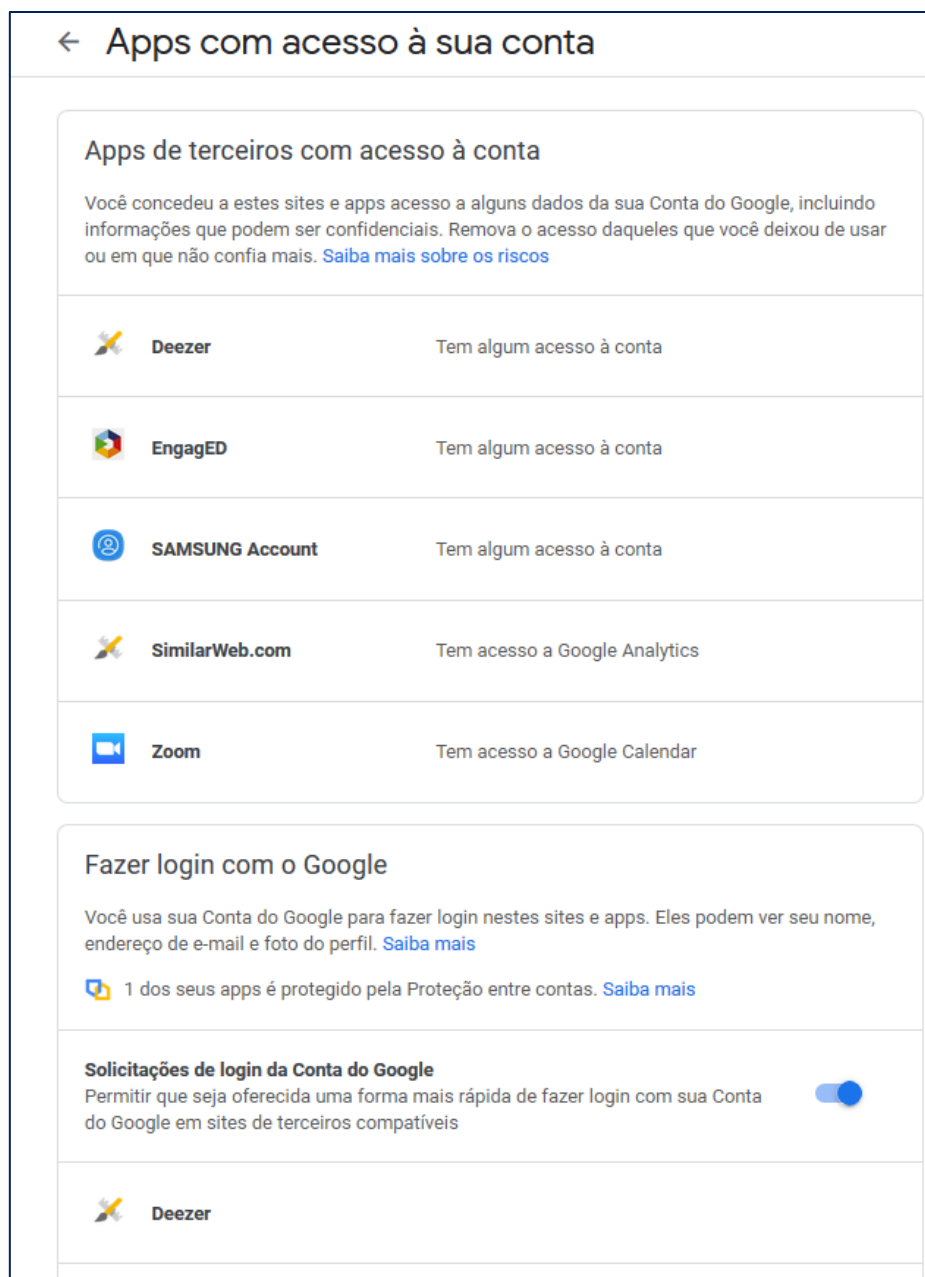
- [Recuperar sua Conta do Google](#) ▾
- [Suspeita de que sua conta foi invadida](#) ▾

Receber ajuda com um produto do Google

Visite nossa [Central de Ajuda e os fóruns de suporte](#).

Fonte: GOOGLE (2020)

O formulário permite apenas que se identifiquem os aplicativos que o titular deu permissões, mas não os fluxos de dados remetidos pelo *Google* a seus parceiros (**Figura 12**).

Figura 12: Apps com acesso à conta *Google*

Fonte: GOOGLE (2020)

Percebe-se que quando se concede permissões dos aplicativos, já ocorre uma transferência de dados aos aplicativos, do mesmo modo, o *Google* tem acesso às atividades dos aplicativos, dados estes que reunidos, podem caracterizar perigoso risco à privacidade dos indivíduos e titulares de dados pessoais. Do mesmo modo, os aplicativos coletam dados que o titular cedeu ao *Google*, e neste momento muitas preocupações devem incidir. Conforme explicita Sant’Anna (2016, p. 6), esta “recuperação” demanda uma séria de questionamentos:

O acesso será feito diretamente a base em que se encontra armazenado ou será necessário retornar a fase de armazenamento para definição de novas estruturas de armazenamento específicas para recuperação? Com que frequência os dados serão atualizados para disponibilização? Quem poderá acessar estes dados? Durante o processo de recuperação quais são os riscos à privacidade dos indivíduos ou entidades referenciados pelos conteúdos recuperados? Como explicitar e operacionalizar a integração entre as diversas estruturas dos dados e destes com outros conjuntos de dados? Como explicitar e garantir os elementos que sustentam a qualidade dos dados que estão sendo disponibilizados? Têm-se o direito de disponibilizar estes dados? Como viabilizar que estes dados sejam encontrados, acessados e passíveis de interpretação (preferencialmente, e em muitos casos obrigatoriamente, por máquinas)? Os processos e procedimentos de recuperação estão estáveis o suficiente para que permaneçam polimorficamente utilizáveis ao longo do tempo? (SANT'ANNA, 2016, p. 6).

E é neste momento que resta demonstrado e claro a necessidade da Ciência da Informação, instrumentalizados pela Ciência da Computação (SANT'ANA, 2016), para que se possa estabelecer um método de descrição adequado e eficaz e que proporcione maior transparência no compartilhamento de dados pessoais.

Não foi possível enviar uma solicitação ao *Google*, pois a página que anuncia “Entrar em contato com o *Google*”⁵ apenas traz respostas pré-prontas. Logo, não se pôde realizar a solicitação de informações sobre compartilhamento de dados.

Não existem descrições dos dados que são compartilhados nem *logs* destas atividades. A *Google* mantém em sua política de privacidade um *link* para uma página “Quem são os parceiros do *Google*”⁶. No entanto, indica apenas que possuem milhões de *sites* e *apps* de terceiros e que os processadores que tratam dados em nome do *Google* são seguros.

O Google trabalha com negócios e organizações de várias maneiras. Nós nos referimos a esses negócios e organizações como "parceiros". Por exemplo, mais de dois milhões de *sites* e *apps* de terceiros fazem parceria com o *Google* para exibir anúncios. Milhões de parceiros desenvolvedores publicam *apps* no *Google Play*. Outros parceiros nos ajudam a proteger nossos serviços. As informações sobre ameaças à segurança podem nos ajudar a notificar você se acreditarmos que sua conta foi comprometida e, então, podemos oferecer assistência com as etapas necessárias para protegê-la.

Na função de "processadores de dados", trabalhamos com empresas confiáveis em vez de parceiros. Essas empresas processam informações em nosso nome, para apoiar nossos serviços, com base em nossas instruções e obedecendo nossa Política de Privacidade e outras medidas de segurança e confidencialidade apropriadas. A Política de Privacidade do *Google* tem mais informações sobre como usamos processadores de dados (GOOGLE, 2020, p. 1).

⁵ https://support.google.com/policies/answer/9581826?p=privpol_privts&hl=pt-BR&visit_id=637265492503235066-2166889955&rd=1

⁶ <https://policies.google.com/privacy/google-partners?hl=pt-BR>

Apresenta apenas alguns parceiros de *COOKIES*, sem informar mais detalhes a respeito (**Figura 13**).

Figura 13: Informações sobre os parceiros de publicidade Google

Informações coletadas ou recebidas pelos parceiros de publicidade do Google

Parceiros específicos, listados abaixo, podem coletar ou receber informações de identificação não pessoais sobre seu navegador ou dispositivo quando você usa apps e sites do Google. Esses parceiros coletam essas informações para fins de publicidade e medição de anúncios usando os próprios cookies ou tecnologias semelhantes.

Por exemplo, permitimos que criadores de conteúdo e anunciantes do YouTube trabalhem com empresas de medição para conhecer o público dos vídeos ou anúncios do YouTube, usando cookies ou tecnologias semelhantes.

Saiba mais sobre como esses parceiros específicos coletam e usam suas informações:

- [Nielsen](#)
- [comScore](#)
- [Integral Ad Science](#)
- [DoubleVerify](#)
- [Oracle Data Cloud](#)
- [Kantar](#)
- [RN SSI Group](#)

O YouTube também permite que os anunciantes e criadores veiculem anúncios diretamente, usando as próprias tecnologias de veiculação de anúncios, fora dos países do EEE.

Fonte: GOOGLE (2020)

4.4 POLÍTICA DE PRIVACIDADE DO *WHATSAPP*

Analisou-se a Política de Privacidade do *WhatsApp*. A Rede *WhatsApp* não apresentou uma central de privacidade, e condensa os itens em “Informações legais do *WhatsApp*”. Neste item existe o *link* para a Política de Privacidade⁷. A Política de Privacidade do *WhatsApp* não é exibida em português.

Foram identificados 26 (vinte e seis) ocorrências para o termo “compartilha” e 40 (quarenta) ocorrências para “transfere” e derivações, incluindo a expressão

⁷ https://www.whatsapp.com/privacy/?lang=pt_br

“transferência”. Sobre os dados que o *WhatsApp* trata de terceiros, é disposto na Política da seguinte forma:

Dados divulgados por terceiros sobre você. Recebemos dados divulgados por outros, o que pode incluir dados sobre você. Por exemplo, quando outros usuários que você conhece utilizam nossos Serviços, eles podem fornecer seu número de telefone que está na agenda de contatos deles (assim como os números deles podem vir de seus contatos); eles podem também enviar-lhe uma mensagem, enviar mensagens para grupos dos quais você participe ou podem ligar para você.

Prestadores de serviço terceirizados. Trabalhamos com prestadores de serviço terceirizados para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços. Por exemplo, trabalhamos com outras empresas para distribuir nossos aplicativos, formar nossos sistemas de infraestrutura, de entrega ou outros, fornecer informações sobre mapas e locais, processar pagamentos, ajudar-nos a entender como as pessoas utilizam nossos Serviços e anunciar nossos Serviços. Esses prestadores de serviço podem nos fornecer informações suas sob determinadas circunstâncias, por exemplo, as lojas de aplicativo podem nos enviar relatórios para nos ajudar a diagnosticar e corrigir problemas no serviço.

Serviços de terceiros. Permitimos o uso de nossos Serviços em conjunto com serviços de terceiros. Se nossos Serviços forem usados com serviços de terceiros, podemos receber dados seus fornecidas por eles, por exemplo, ao usar o botão Compartilhar do *WhatsApp* em um serviço de notícias para compartilhar uma reportagem com seus contatos e grupos do *WhatsApp* ou listas de transmissão de nossos Serviços, ou ao optar por acessar nossos Serviços por meio da promoção feita pela operadora de celular ou pela fornecedora do dispositivo. Observe que ao usar serviços de terceiros, os termos e as políticas de privacidade aplicáveis serão os elaborados para tais serviços (WHATSAPP, 2020, p. 1).

Quanto ao compartilhamento de dados, o *WhatsApp* estabelece que os dados dos usuários são compartilhados à medida em que este se comunica e utiliza os serviços. A rede informa que compartilha os dados pois estes são úteis para ajudá-los a operar, aprimorar, entender, personalizar, dar suporte e promover os serviços (WHATSAPP, 2020). Além dos dados que o próprio usuário opta por compartilhar, a rede informa realizar o compartilhamento com prestadores de serviço terceirizados e serviços de terceiros:

Prestadores de serviço terceirizados. Trabalhamos com prestadores de serviço terceirizados para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços. Quando compartilhamos dados com prestadores de serviço terceirizados, exigimos que eles utilizem seus dados de acordo com nossas instruções e termos ou mediante seu consentimento expresso.

Serviços de terceiros. Quando você usa serviços de terceiros que são integrados aos nossos Serviços, eles podem receber dados sobre seus compartilhamentos. Por exemplo, ao usar um serviço de *backup* de dados integrado aos nossos Serviços (como o *iCloud* ou o *Google Drive*), eles receberão informações sobre o que é compartilhado por você. Ao interagir com um serviço de terceiros conectado com nossos Serviços, você pode acabar

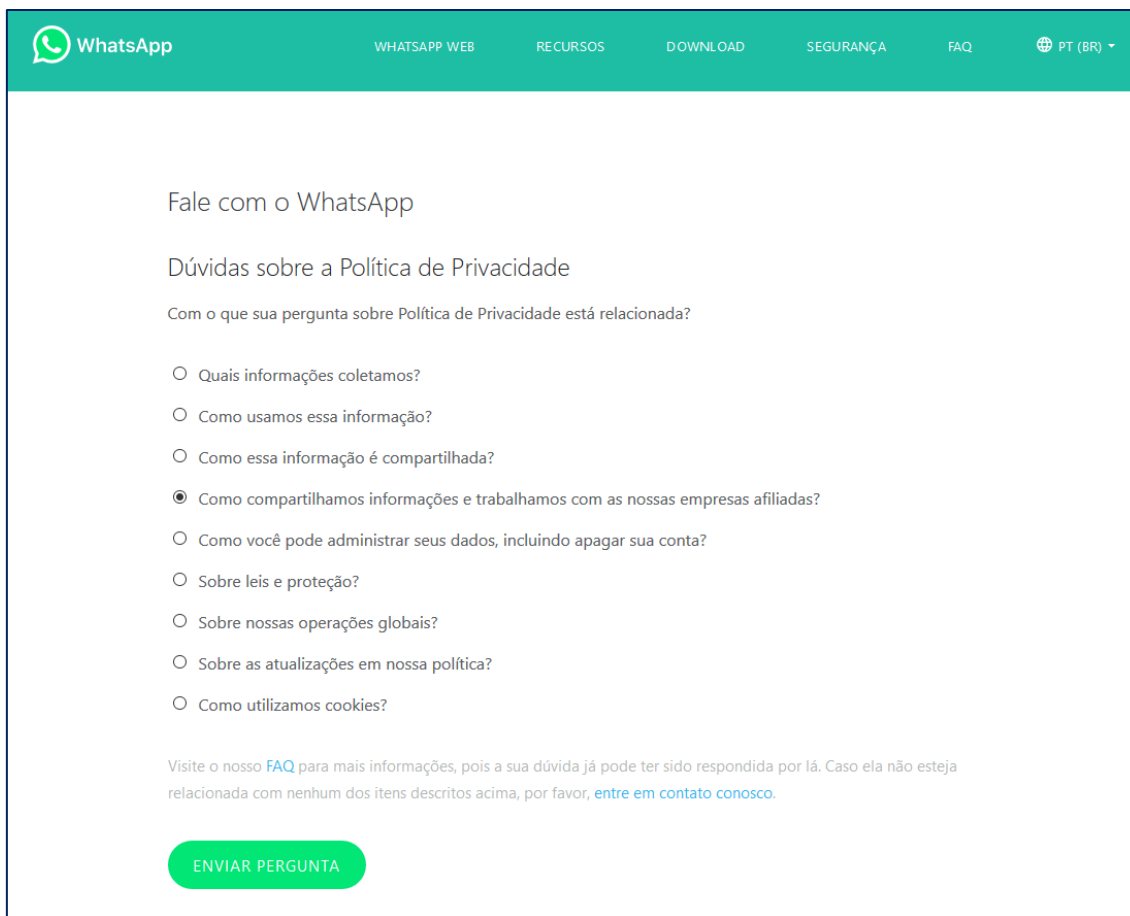
fornecendo dados diretamente a eles. Observe que ao usar serviços de terceiros, os termos e as políticas de privacidade aplicáveis serão os elaborados para tais serviços (WHATSAPP, 2020, p. 1).

No entanto, em nenhum momento especifica quais são estes prestadores de serviços terceirizados ou serviços de terceiros que têm acesso aos referidos dados pessoais. Existe previsão de que os dados podem ser compartilhados para empresas do grupo de empresas que faz parte da família *Facebook*:

Passamos a fazer parte da família de empresas do *Facebook* em 2014. Como parte desta família, o *WhatsApp* recebe e compartilha dados com os demais membros. Podemos usar os dados fornecidos por eles e eles podem usar os dados compartilhados por nós para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços e as ofertas deles. Isso inclui a ajuda no aprimoramento dos sistemas de infraestrutura e entrega, a compreensão de como nossos Serviços ou os serviços deles são usados, a proteção dos sistemas e o combate a spam, abuso ou atividades que violem o uso lícito destes. O *Facebook* e outras empresas do mesmo grupo também podem usar dados do *WhatsApp* para fazer sugestões (por exemplo, de amigos, de contatos ou de conteúdo interessante) e mostrar ofertas e anúncios relevantes. No entanto, suas mensagens do *WhatsApp* permanecem privadas e não serão compartilhadas no *Facebook* para que outros vejam. Na verdade, o *Facebook* não usará suas mensagens do *WhatsApp* por qualquer motivo que não seja nos auxiliar na operação e na execução dos Serviços (WHATSAPP, 2020, p. 1).

Como contato para solicitações, a plataforma disponibiliza um formulário de opções (**Figura 14**). A opção para acesso às operações de compartilhamento, assim como nas demais redes sociais, não é apresentada. Ao clicar em “Como compartilhamos informações e trabalhamos com as nossas empresas afiliadas”, o formulário redireciona para um *e-mail*.

Figura 14: Formulário de contato WhatsApp



WhatsApp

WHATSAPP WEB RECURSOS DOWNLOAD SEGURANÇA FAQ PT (BR)

Fale com o WhatsApp

Dúvidas sobre a Política de Privacidade

Com o que sua pergunta sobre Política de Privacidade está relacionada?

- Quais informações coletamos?
- Como usamos essa informação?
- Como essa informação é compartilhada?
- Como compartilhamos informações e trabalhamos com as nossas empresas afiliadas?
- Como você pode administrar seus dados, incluindo apagar sua conta?
- Sobre leis e proteção?
- Sobre nossas operações globais?
- Sobre as atualizações em nossa política?
- Como utilizamos cookies?

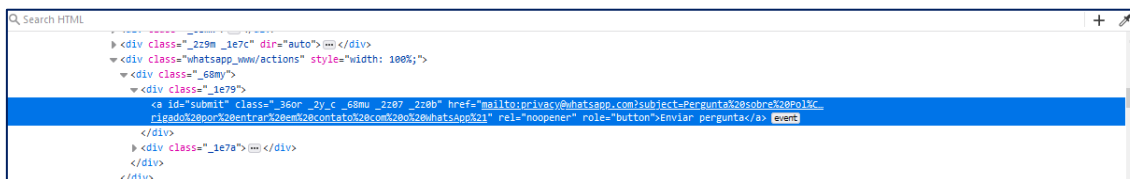
Visite o nosso [FAQ](#) para mais informações, pois a sua dúvida já pode ter sido respondida por lá. Caso ela não esteja relacionada com nenhum dos itens descritos acima, por favor, [entre em contato conosco](#).

ENVIAR PERGUNTA

Fonte: WHATSAPP (2020)

Logo que se clica no botão um *link* para o envio de um *e-mail* é exibido na tela (Figura 15).

Figura 15: Link do botão para o e-mail de privacidade do WhatsApp



```

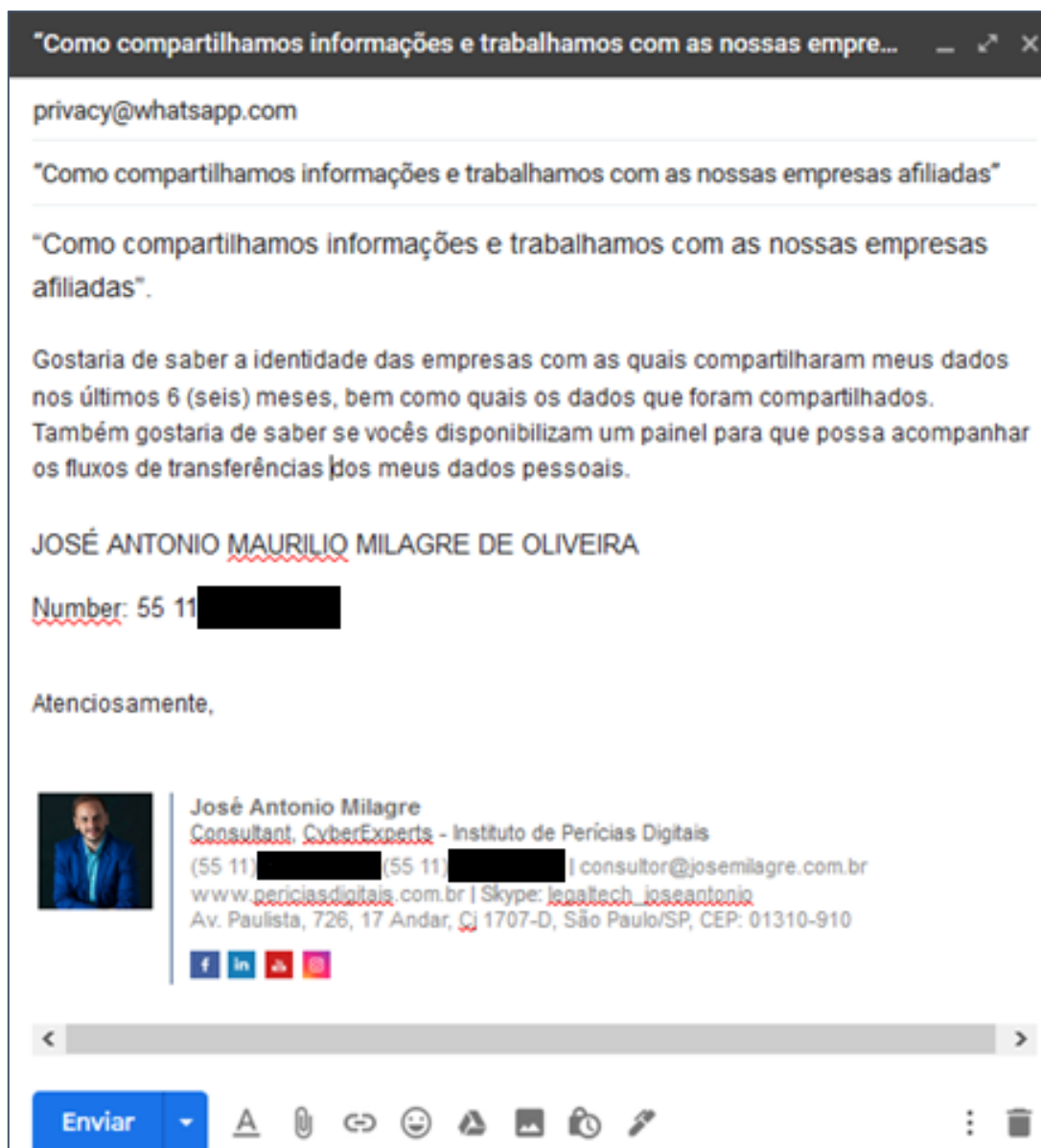
<div class="_2z9m _1e7c" dir="auto"></div>
<div class="whatsapp_www/actions" style="width: 100%;">
  <div class="_68my">
    <div class="_1e79">
      <a id="submit" class="_36or _2y_c _68mu _2z07 _2z0b" href="mailto:privacy@whatsapp.com?subject=Pergunta%20sobre%20pol%C3%ADtica%20de%20privacidade&entry=2&entry2=contato%20com%20o%20whatsapp%21" rel="noopener" role="button">Enviar pergunta</a>
    </div>
  </div>
</div>
<div class="_1e7a"></div>
</div>

```

Fonte: WHATSAPP (2020)

Enviou-se *e-mail* em 31/05/2020, para que a rede pudesse informar, efetivamente, com quais empresas realiza o compartilhamento de dados e quais foram (Figura 16):

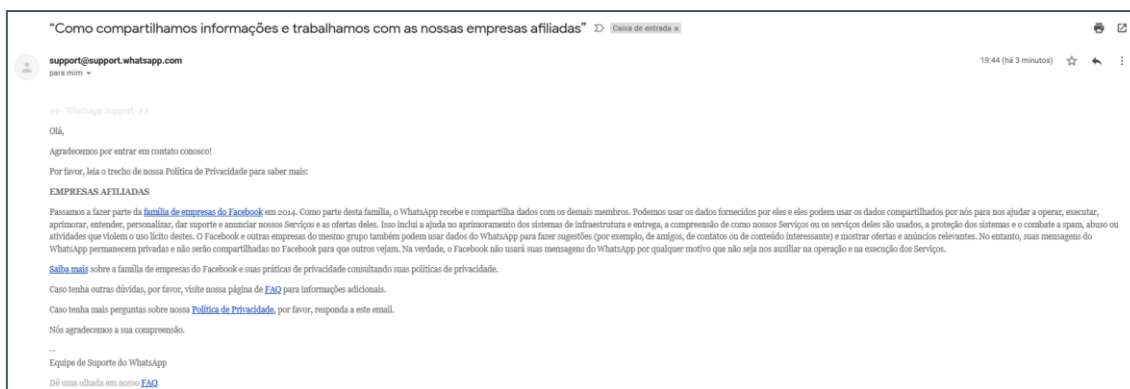
Figura 16: E-mail enviado ao WhatsApp



Fonte: elaborado pelo autor (2020)

O *WhatsApp* respondeu o *e-mail* enviando uma resposta padronizada, alguns minutos depois, e pedindo para que consulte a política de privacidade, que já havia sido revisada (**Figura 17**).

Figura 17: Resposta do *WhatsApp* sobre a solicitação das informações sobre o compartilhamento de dados pessoais



Fonte: elaborado pelo autor (2020)

Como se constatou, o *WhatsApp* não apresenta transparência nas operações de tratamento de dados pessoais. Na política de privacidade, oferece um contato de *e-mail* que, quando é acionado, em resposta, pede para que o titular de dados leia a política, que nada diz a respeito.

4.5 TERMOS DE USO *STRAVA*

O *Strava* é um dos aplicativos mais populares do Público *Fitness*. Embora não tenha uma central de privacidade, nem página específica que trate da Lei Geral de Proteção de Dados pessoais, a Política de Privacidade da *Strava* é resumida em um documento denominado “Tabela de Privacidade” (**Figura 18**). O usuário também pode acessar a política completa, caso prefira.

Figura 18: Tabela de Privacidade *Strava*

Tabela de privacidade	
Coleta e venda de dados	
Nós vendemos suas informações pessoais?	Não
Nós compartilhamos ou vendemos informações agregadas?	Sim
Nós compartilhamos seus dados com parceiros de API?	Sim, com o seu consentimento
Nós usamos categorias de dados confidenciais, como informações de saúde?	Sim, com o seu consentimento
Nós usamos sua lista de contatos, se você permitir nosso acesso?	Sim
Nós excluimos seus dados quando você solicita a exclusão da conta?	Sim
Nós retemos seus dados pelo tempo que for necessário a menos que você solicite exclusão?	Sim
Ferramentas e controle de privacidade	
Você pode controlar quem vê sua atividade e conteúdo?	Sim
Você pode controlar quem vê sua atividade baseada em local?	Sim
Os controles de privacidade são definidos para "Todos" por padrão?	Sim
Você pode baixar e excluir seus dados?	Sim
Todos os usuários no mundo inteiro têm o mesmo conjunto de ferramentas e controles?	Sim
Rastreamento	
Nós rastreamos a localização do seu dispositivo para oferecer o Strava a você?	Sim
Nós rastreamos a localização do seu dispositivo enquanto você não está usando o app?	Não
Nós usamos cookies?	Sim
Nós rastreamos suas atividades de navegação em outros sites?	Não
Nós ouvimos você usando o microfone do seu dispositivo?	Não
Comunicação	
Nós avisamos antes de fazer alterações importantes em nossa Política de privacidade?	Sim
Nós enviamos comunicações de marketing com opção de interromper o recebimento?	Sim
Nós enviamos notificações por push com opção de interromper o recebimento?	Sim

Fonte: STRAVA (2020)

O *Strava* reconhece em sua política de privacidade que realiza o compartilhamento de dados pessoais:

Também usamos as informações que coletamos para analisar, desenvolver e aprimorar os Serviços. Para fazer isso, a *Strava* pode usar provedores de análise de terceiros para obter informações sobre como os nossos Serviços são usados e para nos ajudar a aprimorar os Serviços.

Além disso, podemos usar as informações de coletamos para comercializar e promover os Serviços, as atividades na *Strava* e outros produtos ou serviços

comerciais. Isso inclui personalizar sua experiência na *Strava*. Por exemplo, se soubermos que você gosta de correr, podemos informá-lo sobre novas atividades de corrida ou mostrar conteúdo patrocinado relacionado a corrida. Se observarmos que você corre em uma determinada área, podemos sugerir uma competição de corrida nessa área. Conforme as suas configurações, também podemos mencionar que você usou os produtos ou serviços de nossos parceiros como parte das suas atividades, o que chamamos de Integrações patrocinadas (STRAVA, 2020, p. 1).

A aplicação também informa a possibilidade de compartilhamento de “informações agregadas”, que estariam fora do conceito de “dados pessoais”. Estas informações podem ser utilizadas para aprimoramento de outros serviços oferecidos pelo aplicativo.

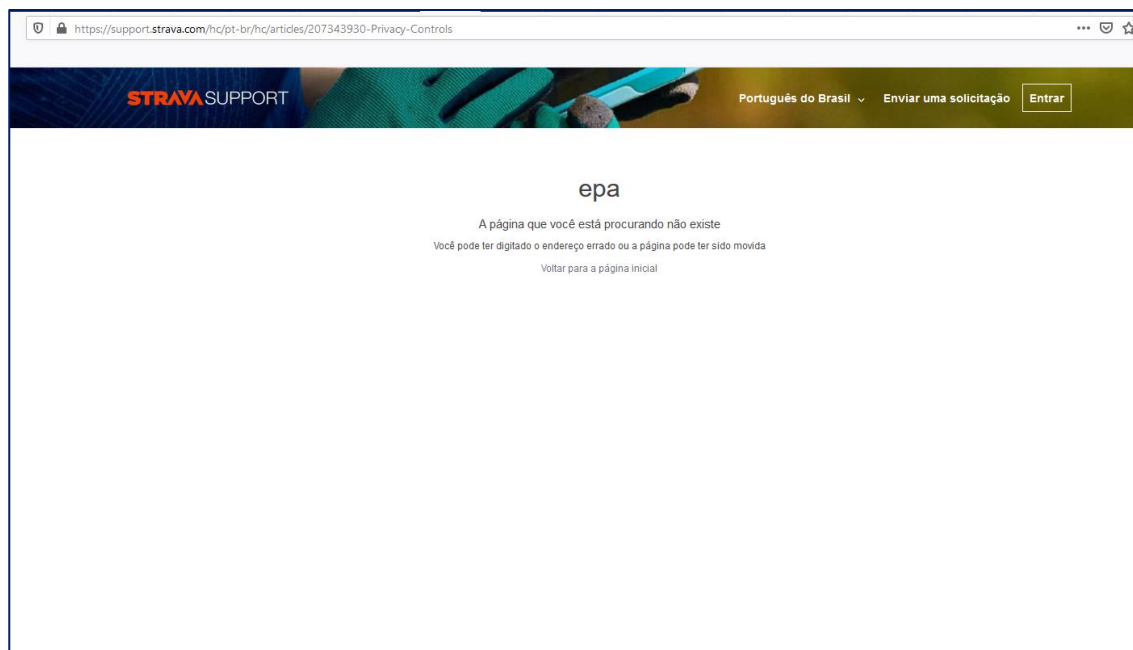
Nós não vendemos suas informações pessoais. A *Strava* pode agregar as informações que você e outras pessoas disponibilizam com relação aos Serviços e publicá-las ao público ou compartilhá-las com terceiros. Exemplos do tipo de informações que podemos agregar incluem informações sobre equipamento, uso, demografia, rotas e desempenho. A *Strava* pode usar, vender, licenciar e compartilhar essas informações agregadas a terceiros para pesquisa, negócios e outros fins, como para aprimorar caminhadas, corridas ou atividades de ciclismo em cidades por meio do *Strava* Metro ou para ajudar nossos parceiros a entender mais sobre os atletas, inclusive as pessoas que usam seus produtos e serviços. A *Strava* também usa dados agregados para gerar nosso Mapa de calor global. Visite seus controles de privacidade, caso se oponha à *Strava* usar suas informações para esses fins (STRAVA, 2020, p. 1).

No que diz respeito aos dados pessoais, a aplicação é clara em sua política ao prever que compartilha dados com provedores de serviços, informações publicamente disponíveis, compartilhamento de informações e atividades, negócios de terceiros por API ou outras integrações, afiliadas ou adquirentes dos negócios e ativos do *Strava* e diante de requisitos legais (STRAVA, 2020).

No entanto, não são especificados quais são estes parceiros e o detalhamento dos dados que são compartilhados. Tentou-se enviar uma solicitação sobre dados compartilhados para o endereço⁸, mas a página estava com falha e não foi exibida (**Figura 19**):

⁸ <https://support.strava.com/hc/pt-br/hc/articles/207343930-Privacy-Controls>

Figura 19: Página de Privacidade do *Strava* é inexistente



Fonte: STRAVA (2020)

4.6 POLÍTICA DE PRIVACIDADE *SAMSUNG* PARA *SMARTVS*

A política de privacidade da *Samsung* trata o compartilhamento de dados como “partilha de dados”. Existe uma política de privacidade geral e uma política para dispositivos “*Smart*”. A empresa informa que compartilha dados com afiliadas, parceiros de negócio, prestadores de serviços, outras entidades, quando requerido por lei ou conforme necessário para proteger os serviços, outras entidades associadas a transações empresariais, outras entidades com o consentimento ou mediante indicação do utilizador.

A quem divulgamos os dados do utilizador?

Não divulgamos os dados do utilizador a terceiros para as suas próprias campanhas de marketing ou fins comerciais independentes sem o consentimento do utilizador. No entanto, podemos divulgar os dados do utilizador às seguintes entidades:

Afiliadas. Caso necessário, os dados do utilizador podem ser partilhados entre as afiliadas da *Samsung*.

Parceiros de negócio. Também podemos partilhar os dados do utilizador com parceiros de negócio de confiança, incluindo operadoras de comunicação sem fios. Estas entidades podem utilizar os dados do utilizador para prestar serviços que tenham sido solicitados pelo mesmo (por exemplo, conteúdo de vídeo fornecidos pela *Netflix* através de *SmartTV*) e prever os interesses do utilizador, podendo enviar ao utilizador materiais promocionais, anúncios publicitários e outros materiais.

Prestadores de serviços. Podemos também divulgar os dados do utilizador a empresas que nos prestem serviços ou que prestem serviços em nosso nome, tais como empresas que nos ajudem na facturação ou que enviem mensagens de e-mail em nosso nome. Estas entidades dispõem de capacidades limitadas

para utilizar os dados do utilizador para finalidades que não sejam as de prestação de serviços por nós.

Outras entidades, quando requerido por lei ou conforme necessário para proteger os nossos Serviços. Podem ocorrer situações em que divulguemos os dados do utilizador a outras entidades para:

Cumprir a lei, ou responder a um processo judicial obrigatório (como um mandato de busca ou outras ordens do tribunal);

Verificar ou assegurar a conformidade com as políticas que regem os nossos Serviços; e

Proteger os direitos ou segurança da *Samsung*, ou de qualquer das respectivas afiliadas.

Outras entidades associadas a transações empresariais. Podemos divulgar os dados do utilizador a terceiros no âmbito de um processo de fusão ou transferência, ou em caso de falência.

Outras entidades com o consentimento ou mediante indicação do utilizador. Para além das divulgações descritas nesta Política de Privacidade, podemos partilhar dados sobre o utilizador com terceiros quando o utilizador consentir ou solicitar tal partilha (SAMSUNG, 2020, p. 1).

Foram identificadas 10 (dez) ocorrências para o termo “partilha” e 7 (sete) ocorrências para a expressão “transferência”. A política disponibiliza um endereço físico para contato e uma página para dúvidas em relação a proteção de dados pessoais⁹. A empresa também disponibiliza uma política específica para *SmartTvs*, que assim define o compartilhamento de dados:

A *Samsung* recolhe, utiliza, partilha e armazena informações através da *Smart TV* do Cliente sob as formas descritas na Política de Privacidade da *Samsung*. Este Suplemento fornece detalhes adicionais sobre as práticas de privacidade de algumas funcionalidades da *Smart TV* (SAMSUNG, 2020, p. 1).

A programação e recomendações da *Samsung* se dão com base nas atividades que o titular de dados faz na TV, incluindo *cookies* e *sites* acessados. No que diz respeito ao compartilhamento com terceiros, a política informa que:

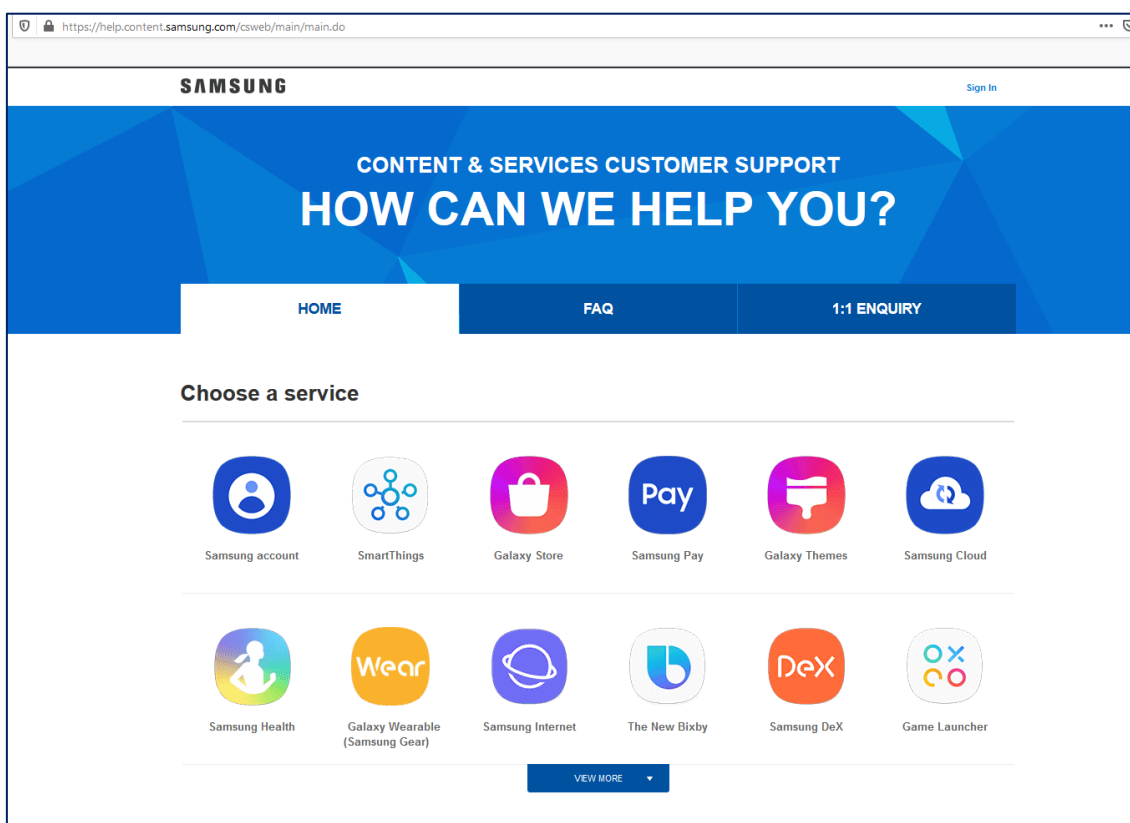
Terceiros

É de salientar que, quando o Cliente vê um vídeo ou acede a aplicações ou conteúdo fornecido por terceiros, esse fornecedor poderá recolher ou receber informações sobre a *Smart TV* (por exemplo, o endereço IP e os identificadores do dispositivo), a transação pedida (por exemplo, o pedido do Cliente para comprar ou alugar o vídeo) e a utilização que o Cliente faz da aplicação ou serviço. A *Samsung* não é responsável pelas práticas de privacidade ou segurança destes fornecedores. O Cliente deverá ser prudente e rever as declarações de privacidade aplicáveis aos *Web sites* e serviços de terceiros utilizados pelo mesmo (SAMSUNG, 2020, p. 1).

Tentou-se fazer contato com a *Samsung* por meio da página indicada pela empresa para requerimento de informações relativas à privacidade. No entanto, a página não oferece opções neste sentido (**Figura 20**):

⁹ <http://help.content.samsung.com>

Figura 20: Página para contato prevista na política de privacidade da Samsung



Fonte: SAMSUNG (2020)

4.7 AVALIAÇÃO DA EXISTÊNCIA DE REGISTROS DE TRANSFERÊNCIA E DA TRANSPARÊNCIA OFERECIDA AO TITULAR DOS DADOS

Como se constatou da análise das aplicações nesta pesquisa, pontos são considerados prejudiciais para obtenção de transparência nos processos de compartilhamento de dados e estão diretamente ligados à organização e descrição das informações a respeito da privacidade dos titulares:

- a) **Central de privacidade:** apenas 2 (duas) aplicações (*Facebook* e *Google*) apresentaram central de Privacidade, página que concentra todas as políticas e opções ao titular de dados;
- b) **Nomenclatura e terminologia diversa:** o *Facebook* utiliza o termo “Política de Dados” para sua política de privacidade, ao contrário das demais redes, que utilizam “Política de Privacidade”. Isto constitui uma dificuldade ao titular em identificar rapidamente seus direitos; somente o *Facebook* disponibiliza uma página sobre a Lei Geral de Proteção de Dados;

- c) **Nomes distintos para mesmas operações:** nas políticas, as expressões “transferência”, “partilha” e “compartilhamento” foram encontradas para designar o compartilhamento de dados pessoais. Esta heterogeneidade também dificulta a transparência ao leitor dos documentos;
- d) **Contatos com as redes:** com exceção do *Google*, todas as demais redes indicam endereços físicos e contatos *online* para questionamentos sobre privacidade;
- e) **Nomes dos agentes com quem os dados são compartilhados:** Nenhuma das redes descreve os nomes dos parceiros e agentes com quem compartilham os dados; todas as redes descrevem “categorias” de parceiros com quem compartilham os dados;
- f) **Registros das transferências:** nenhuma das redes oferece aos titulares a possibilidade de terem acesso os registros das atividades e compartilhamento;
- g) **Descrição dos dados compartilhados:** nenhuma das redes oferece aos titulares a de possibilidade verificarem quais dados são transferidos;
- h) **Formulários para contato:** embora todas as redes digam que disponibilizam um ponto de contato para que o titular possa requerer direitos ou informações, em 3 (três) das 5 (cinco) redes analisadas não foi possível sequer fazer a solicitação: *Google*, *Strava* e *Samsung*;
- i) **Resposta dos contatos:** para as 2 (duas) aplicações que permitiram contato para mais informações e esclarecimentos sobre transferência de dados pessoais, *Facebook* não respondeu a mensagem enviada, e *WhatsApp* respondeu com uma mensagem “padrão”, alguns minutos depois, sem que fosse esclarecido com quem compartilha dados pessoais e quais são os dados compartilhados.

A seguir é apresentada avaliação da transparência das aplicações sobre compartilhamento de dados pessoais (**Quadro 11**).

Quadro 11: Avaliação da transparência das aplicações sobre compartilhamento de dados pessoais

	Rede Social	Facebook	Google	WhatsApp	Samsung	Strava
1	Data da análise	05/04/2020	23/04/2020	01/05/2020	15/05/2020	31/05/2020
2	Central de Privacidade	https://www.facebook.com/privacy/	https://policies.google.com/privacy	Não possui	Não possui	Não possui
3	Política de Privacidade	Não apresenta	https://www.gstatic.com/policies/privacy/pdf/20200331/acec359e/google_privacy_policy_pt-BR.pdf	https://www.whatsapp.com/legal/?lang=pt_pt#privacy-policy	https://www.samsung.com/africa/pt/info/privacy/	https://www.strava.com/legal/privacy?hl=pt-BR
4	Política de Dados	https://www.facebook.com/policy.php	Não apresenta	Não apresenta	Não apresenta	Não apresenta
5	Termos de uso	https://www.facebook.com/terms/	https://policies.google.com/terms?hl=pt-BR	https://www.whatsapp.com/legal/?lang=pt_pt#terms-of-service	Não possui	https://www.strava.com/legal/terms
6	Página leis de proteção de dados	https://www.facebook.com/business/gdpr	Não apresenta	Não apresenta	Não apresenta	Não apresenta
7	Termos "compartilha"	45	30	26	10	33
11	Como definem transferência	A rede social estabelece a possibilidade de compartilhamento de dados com parceiros externos, parceiros que usam o serviço de análise, anunciantes, parceiros de mensuração, parceiros que oferecem bens e serviços em nossos produtos, fornecedores e provedores de serviços, pesquisadores e acadêmicos, aplicação da lei ou solicitações legais.	Informam que não compartilham dados pessoais, porém trazem quatro exceções: o consentimento, com administradores de domínio, para processamento externo e por motivos legais. Ainda prevêem a possibilidade de cessão de dados anonimizados.	Informa que compartilha dados pessoais com prestadores de serviços terceirizados e para serviços de terceiros, que são integrados aos serviços. Não indicam quem são estes parceiros ou terceiros	A empresa informa que compartilha dados com afiliadas, parceiros de negócio, prestadores de serviços, outras entidades, quando requerido por lei ou conforme necessário para proteger os serviços, outras entidades associadas a transações empresariais, outras entidades com o consentimento ou mediante indicação do utilizador	A aplicação é clara em sua política ao prever que compartilha dados com provedores de serviços, informações publicamente disponíveis, compartilhamento de informações e atividades, negócios de terceiros por API ou outras integrações, afiliadas ou adquirentes dos negócios e ativos do Strava e diante de requisitos legais
9	Termos transferência	6	5	40	7	3
10	Contato para solicitações	Endereço físico e contato online	Contato online	Endereço físico e contato online	Endereço físico e contato online	Endereço físico e contato online
11	Informam nomes dos processadores	Não	Não	Não	Não	Não
12	Logs de transferências	Não	Não	Não	Não	Não
13	Descrição de dados	Não	Não	Não	Não	Não
14	Formulário de contato	https://www.facebook.com/help/contact/861937627253138	https://support.google.com/policies?p=privacy_privts&hl=pt_BR	https://www.whatsapp.com/contact/?subject=privacy	http://help.content.samsung.com	https://support.strava.com/
15	Resposta	Não	Não é possível contatar	Sim, automatizada	Não é possível contatar	Não é possível contatar
16	Observações	Saiba mais sobre como controlar as informações pessoais que você ou outras pessoas compartilham com parceiros externos nas Configurações do Facebook e do Instagram	A Google possui uma seção "Quem são os parceiros do Google". Mas a seção não indica quais os terceiros e processadores que recebem dados pessoais dos usuários. Apresenta apenas alguns parceiros de "cookies"	Permite contato por meio de um e-mail privacy@whatsapp.com para que pessoas tirem dúvidas sobre compartilhamento de dados	A empresa disponibiliza uma política específica para Smartv em https://www.samsung.com/br/info/privacy/smartv/ onde informa que transfere dados a terceiros	A página para contato sobre questões de privacidade estava inativa.
17	Última revisão	19/04/2018	31/03/2020	28/01/2020	21/04/2017	11/12/2019

Fonte: elaborado pelo autor (2020)

Analisou-se a Política de Privacidade de 5 (cinco) aplicações, de modo a identificar como tratam e endereçam a questão envolvendo a transparência nas operações de compartilhamento. Os resultados, conforme evidenciados no **Quadro 11** (p. 112), demonstram riscos gravíssimos à privacidade e aos direitos dos titulares dos dados.

Como se verificou, além dos problemas envolvendo nomenclaturas diversas, com exceção do *Google*, todas as demais redes indicam endereços físicos e contatos *online* para questionamentos sobre privacidade.

Por outro lado, embora “asseguem” e prevejam nas políticas as atividades de compartilhamento de dados, nenhuma das redes descreve os nomes dos parceiros e agentes com quem compartilham os dados; todas as redes descrevem “categorias” de parceiros com quem compartilham os dados, por demais genérico, não identificando quem são as pessoas ou empresas.

Do mesmo modo, não foi identificado em 100% (cem por cento) das redes analisadas a possibilidade de titulares acessarem os registros das atividades e compartilhamento, tampouco os dados compartilhados e como são descritos.

Como fora identificado, embora todas as redes informem que disponibilizam um ponto de contato para que o titular possa requerer direitos ou informações, em 3 (três) das 5 (cinco) redes analisadas não foi possível sequer fazer a solicitação: *Google*, *Strava* e *Samsung*, pois os *links* de contato levam a páginas informativas e não, realmente, a formulários ou pontos de contato.

Para as 2 (duas) aplicações que permitiram contato para mais informações e esclarecimentos sobre transferência de dados pessoais, *Facebook* não respondeu a mensagem enviada, e *WhatsApp* respondeu com uma mensagem “padrão”, alguns minutos depois, sem que fosse esclarecido com quem compartilha dados pessoais e quais são os dados compartilhados.

Deste modo, este é um cenário de extremo risco aos titulares de dados, de maneira que não se pode afirmar que as aplicações estão em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e *General Data Protection Regulation* (GDPR).

Este ambiente, de extrema ausência de transparência, centralizado e assimétrico, e onde os titulares de dados não têm conhecimento sobre a existência ou não de compartilhamentos e para quais empresas, nitidamente potencializa o poder dos controladores e faz com que os titulares percam o controle sobre seus dados (MAYER-SCHÖNBERGER, 2011).

Assim, avaliando-se as disposições, princípios e garantias previstos na legislação Brasileira e Europeia, bem como após revisão dos códigos e boas práticas identificados para compartilhamento de dados e como as aplicações tratam estas informações, resta claro que a forma com que as redes estão tratando o compartilhamento de dados pessoais atualmente revela-se prejudicial aos direitos dos titulares e, apesar da legislação em vigor, um forte atentado a privacidade dos indivíduos. Na busca para suprir esta obscuridade perigosa aos direitos fundamentais envolvendo proteção de dados pessoais, apresenta-se a revisão das pesquisas envolvendo *Blockchain* e como pode esta tecnologia descentralizada contribuir para o aprimoramento da transparência e privacidade de dados, como base para um modelo de registro de operações de compartilhamento de dados pessoais.

5 A *BLOCKCHAIN*, DESCENTRALIZAÇÃO E DESAFIOS NA PROTEÇÃO A DADOS PESSOAIS

A *Blockchain* é uma tecnologia relativamente nova, também conhecida como *Distributed Ledger Technology* (DLT). Proposta em 2018 por Satoshi Nakamoto, que concebeu o conceito de uma criptomoeda denominada “*Bitcoin*” (NAKAMOTO, 2008), um ativo digital que funcionasse em uma rede *peer-to-peer* (P2P) que permitisse o envio de pagamentos *online* de forma segura e sem a necessidade de intermediários (instituições bancárias). Deste modo, fora concebido um sistema econômico, eficiente, confiável e seguro para registrar transações financeiras (CRUZ, 2018). No entanto, após a concepção de suporte para transações financeiras, pesquisadores perceberam que a tecnologia poderia servir de base para registros de outros dados:

Após a implantação das primeiras criptomoedas, vários especialistas observaram que propriedades intrínsecas à tecnologia *Blockchain* (tais como segurança, resiliência, inviolabilidade e imutabilidade) poderiam ser usadas em vários outros tipos de aplicações. Neste sentido, as plataformas de desenvolvimento *Blockchain* evoluíram e permitiram a inserção de transações mais complexas através dos contratos inteligentes (*smart contracts*) (FORMIGONI; BRAGA; LEAL, 2017, p. 3).

Quando se trata de privacidade e *Blockchain*, um dos pontos focais das pesquisas relaciona as transações na *Blockchain* como seguras e privadas. Por outro lado, questões de revelação ou exposição da privacidade são levantadas nas pesquisas científicas. Para *Blockchains* públicas, ferramentas de estatísticas como análises de grafos, em combinação com *web-scrapers*, são utilizadas para identificar os titulares de carteiras *Bitcoins* e suas chaves privadas (SCHWERIN, 2018).

A relevância da *Blockchain* em um cenário de regulamentos de proteção de dados é apresentada pela pesquisa. Fabiano (2018) aborda o crescimento da Internet das coisas (IoT) nos lares das pessoas, integradas com inteligência artificial para a tomada de decisões e realizando o tratamento de dados pessoais diariamente, advertindo para o risco relativo aos dados pois, se os objetos são conectados aos dados sobre as pessoas através das informações que são transmitidas por estes objetos pela Internet, pode-se constituir em risco, destacando que na Europa, a Carta de Direitos Fundamentais estabelece em seu artigo 7º a privacidade como um dos direitos fundamentais.

Neste sentido, a privacidade da *Blockchain* poderia ser mantida se as pessoas mantiverem as chaves anônimas, pois o risco pode ocorrer se o proprietário de uma chave é revelado, o que pode revelar vínculos de transações deste proprietário, sendo possível

rastrear sua interação com serviços *web*, gravada no livro razão sobretudo em uma rede pública, onde os pontos que integram à rede (denominado “*nodos*”) não tem controles sobre seus próprios atos.

Para isso, Fabiano (2018, p. 4) recomenda o uso da *Blockchain Privada*:

Na *blockchain* privada, em vez disso, a privacidade e os dados lei de proteção será aplicada à organização e conseqüentemente, deve-se respeitar todas as obrigações legais, incluindo as informações ao titular dos dados, seu consentimento e direitos. No entanto, é altamente recomendável configurar a privacidade e políticas de segurança.

Eichler *et al.* (2018) tratam dos impactos das tecnologias descentralizadas, como a *Blockchain*, na questão envolvendo a proteção de dados e necessidade dos regulamentos compreenderem esta arquitetura. Aplicar as leis de proteção de dados neste ambiente é muito difícil, considerando que não sabe quem é o usuário (titular dos dados) e quem é o servidor (controlador dos dados). A preocupação sobre a possível adequação da *Blockchain* à *General Data Protection Regulation* (GDPR) pode se caracterizar em relação aos seguintes dados:

- a) Par de chaves: a estrutura de autenticação na *Blockchain* se dá através de um par de chaves, sendo que a pública é tipicamente visível. Tal fato poderia permitir a identificação de proprietários das chaves pública e conseqüentemente a violação de dados pessoais. A pesquisa identifica que se a chave pública está ligada a outra entidade não pode ser considerada dado pessoal;
- b) Outros dados armazenados: a *Blockchain* pode armazenar outros dados, além do que simples transações financeiras, e dados pessoais podem ser gravados em estruturas públicas e permanecerem expostos, de forma indelével.

Uma alternativa para a gravação de dados na *Blockchain* seria a utilização de *hashed data*, a aplicação de algoritmos aplicados em *datastes*, de qualquer tamanho, para gerar uma *string* de tamanho fixo. A função de *hashing* pode servir para se averiguar a integridade de um *dataset*, para se ofuscar um texto plano, o que poderia expor dados pessoais, além de contornar as limitações de tamanho dos dados, que podem ser gravadas em uma simples transação, o que atenderia o requisito de pseudonimização previsto por autoridades e grupos de proteção de dados, como o *Working Party 29*, esclarecendo, igualmente, que a criptografia é considerada pseudonimização e não anonimização, sendo esta recomendada (EICHLER *et al.*, 2018).

Uma proposta para utilizar a *Blockchain* para “registrar” dados sem expor a privacidade dos titulares dos dados seria a utilização da sistemática *Zero Knowledge System* (EICHLER *et al.*, 2018), onde, a partir dela, o controlador de dados pode demonstrar que possui os dados, ou que transacionou com os dados sem expô-los em si, como no exemplo de carteiras que não gravam dados de transações na *Blockchain* (quem ganhou, quem recebeu, quantidade), mas somente a realização da transação.

Ponto que também necessita ser discutido nas transações que utilizam de base a plataforma *Blockchain* é sua característica de imutabilidade, o que poderia conflitar com o disposto na Lei Geral de Proteção de Dados e *General Data Protection Regulation* que garantem ao titular, por exemplo, o direito a retificação e exclusão de dados.

Como estratégias para contar este cenário estariam a anonimização e, caso ocorra a construção de aplicações na *Blockchain* pública, que sejam observados os princípios de privacidade por design, considerando a minimização e avaliação dos impactos e riscos de se gravar dados pessoais na *Blockchain* de forma indelével.

No ponto de vista da *Bundesblock*, a *hash* data pode ser aceitável em circunstâncias em que é garantido de que os dados não podem ser reconstruídos; armazenamento de dados criptografados é muito arriscado, pois a criptografia pode ser quebrada futuramente (EICHLER *et al.*, 2018, p. 4, tradução nossa).

Do mesmo modo, ao tratar sobre os aparentes conflitos e problemas de privacidade envolvendo a *Blockchain* e sua harmonização com as legislações de proteção de dados, Filippone (2017) afirma que, se por um lado a *Blockchain* pode gerar aos indivíduos mais privacidade e autonomia do que em sistemas centralizados, por outro lado os desafios para não tornar a tecnologia intrusiva são muitos. Neste sentido, a descrição formal de dados poderá contribuir, assim como a anonimização, pseudonimização e criptografia, no sentido de atenuar este cenário.

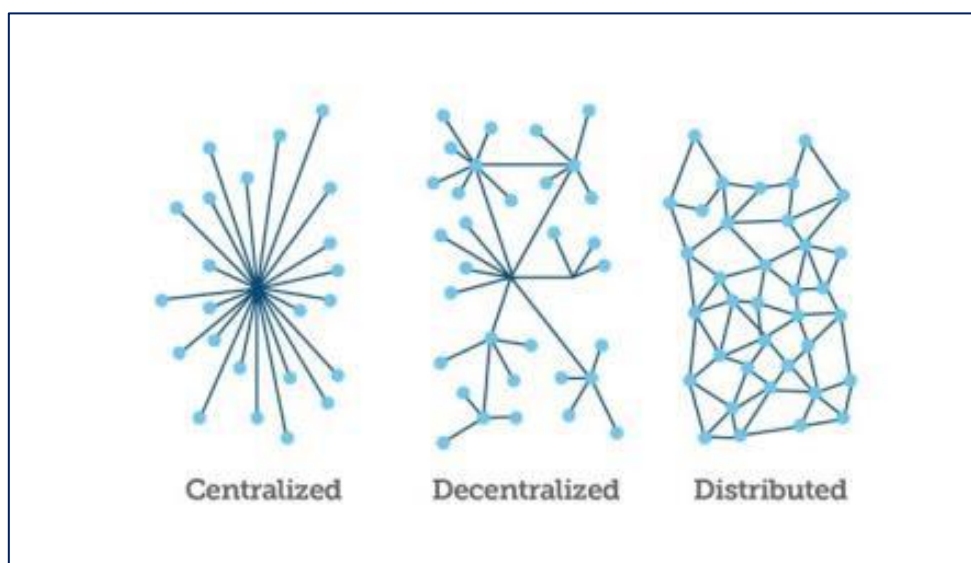
Ao tratar sobre a centralização, o autor explicita o papel trágico para a privacidade dos titulares de dados pessoais:

As plataformas centralizadas, por design, coletam informações sobre a atividade *online* dos usuários. De fato, como visto no Capítulo I, os dados pessoais representam um aspecto central da economia digital e sua concentração nas mãos de um jogador aumenta o poder daqueles que, legitimamente ou não, exercem controle sobre os lucros dos dados, profundo conhecimento das tendências de compra dos clientes, anúncios comportamentais etc. Sempre que uma atividade que requer intermediários centrais é realizada, a posição de poder e os lucros relacionados são reafirmados. Um dos principais benefícios da falta de um ponto central de controle sobre o fluxo de informações da rede é que a vigilância é mais difícil de ser alcançada. Na *blockchain*, de fato, não há uma parte central com controle

estendido sobre os dados de indivíduos decorrentes de atividades de armazenamento e processamento. Esse design deve ser benéfico para o controle de seus usuários sobre seus dados, porque eles não precisam temer a concentração de seus dados e a possível criação de perfil por terceiros que prestam o serviço. Com uma arquitetura altamente descentralizada como *blockchain*, o panóptico digital não deve ocorrer devido à falta de um ponto central de controle em sua arquitetura (FILIPPONE, 2017, p. 28, tradução nossa).

Na **Figura 21** são apresentadas as tecnologias distribuídas utilizadas na *Blockchain*.

Figura 21: Tecnologia Distribuída utilizada na *Blockchain*



Fonte: FILIPPONE (2017, p. 28)

A descentralização também favorece o maior controle dos titulares em relação a seus dados pessoais, pela característica da “transparência”. Na *Blockchain* os participantes sabem quais dados são coletados sobre si próprios e todas as transações ficam registradas na rede, sendo que qualquer modificação neste protocolo requererá o consenso da maioria da rede.

Apesar da suposta privacidade e combinação de critérios de criptografia e pseudonimização, os autores também alertam para a existência de ferramentas que podem, hoje, percorrendo a *Blockchain*, associar pseudônimos a identidades reais, retroativamente reconstruindo o histórico de transações dos titulares.

No que diz respeito aos dados que são gravados na *Blockchain* serem considerados dados pessoais, apesar da identidade dos titulares serem cobertas pela plataforma, a transparência da *Blockchain* exige necessariamente alguns metadados, como endereço dos envolvidos, tamanho, tempo e o tipo de transação, o que se amoldaria claramente no

conceito de dados pessoais, tanto na *General Data Protection Regulation* como na *Lei Geral de Proteção de Dados*.

GDPR (2020, p. 1):

Artigo 4

Definições

Para efeitos do presente regulamento, entende-se por:

- (1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

LGPD (BRASIL, 2018, p. 1):

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

O endereço que aparece em uma transação na *Blockchain* é considerado uma pseudonimização, esta que não retira o caráter do dado de “dado pessoal”, já que “somente torna dificultoso identificar o titular dos dados, mas não impossível” (FILIPPONE, 2017, p. 32).

Como se constata, ao se avaliar os pontos contrários de se armazenar dados na *Blockchain*, identifica-se um problema em relação ao exercício de direitos, como por exemplo as limitações previstas na legislação para que ocorra somente e tão somente a coleta e tratamento do que for necessário para um tipo de tratamento de dados. Considerando que a rede envia cópia dos dados para outros pontos, pode se tornar dificultoso em um cenário de limitações e de processadores incertos. O mesmo problema pode ocorrer com o direito ao apagamento e retificação.

Diante dos riscos, o que poderia ser gravado são dados que asseguram que ocorreu uma transação sem, contudo, identificar para quais atores ou quem é o titular dos dados, metadados que equilibrassem a privacidade do titular e ao mesmo tempo ampliasse seu direito de conhecer as operações de tratamento e compartilhamento que são realizadas com seus dados.

Acerca dos riscos da *Blockchain* pública, tem-se também o risco de uma governança duvidosa que possa estabelecer novos controladores ocultos da informação.

Além disso, a governança da *blockchain* é altamente controversa devido às tendências de centralização que podem dar origem a novas formas de elites não

oficiais controlando o sistema, mas sem legitimidade. Se não for regulamentada, a *blockchain* pode replicar o que aconteceu com a Internet que, de um espaço descentralizado, se transformou em uma centralizada nas mãos de empresas poderosas. Além disso, a governança da *blockchain* é altamente controversa devido às tendências de centralização que podem dar origem a novas formas de elites não oficiais controlando o sistema, mas sem legitimidade (FILIPPONE, 2017, p. 36, tradução nossa).

Os autores concluem informando que uma solução centralizada em *compliance* com GDPR pode ser melhor do que uma solução descentralizada onde seu design mantém indivíduos desprotegidos e nas mãos de “*techno-elites*” com energias desconhecidas.

A *Blockchain*, igualmente, possibilitou o desenvolvimento de outros protocolos, e *frameworks* que permitem o desenvolvimento de outras aplicações de *softwares* descentralizados, como a *Ethereum* (BUTERIN, 2013). *Smart Contract* é definido como um programa computacional auto executado na *Blockchain*, baseado na ocorrência de condições (SZABO, 1997), sendo que em 2015, a *Ethereum* se tornou a primeira real implementação do conceito de contratos inteligentes.

Sater (2017) define que com a proliferação da Internet, conectividades e novas tecnologias, dados pessoais estão sendo constantemente capturados e, neste sentido, as leis estão respondendo, como a *General Data Protection Regulation*. A *Blockchain* pode facilitar este cenário criando um ambiente seguro para troca de informações, através de livro distribuído, transações seguras e modelos de consenso.

Por meio de contratos inteligentes, as organizações podem usar, produzir e distribuir dados através dos limites, garantindo que os dados permaneçam atualizados e preciso em todos os nós. Os controles de acesso da *blockchain* permitiriam aos auditores a capacidade na rede para garantir que os participantes sejam honestos e estejam em conformidade (SATER, 2017, p. 30, tradução nossa).

O autor propõe a criação de um consórcio *Blockchain* em conformidade com o cenário regulatório, que permitirá às empresas compartilharem dados através do mundo, sem preocupações e o que pode cooperar para um padrão de armazenamento de dados, permitindo um painel para que os usuários possam rastrear seus dados, por meio de IDs digitais, estabelecendo ainda que, se a GDPR exige que os sistemas sejam *privacy by design*, a *Blockchain* é *privacy by design*, considerando inúmeras iniciativas, surgindo para Identidade digital, como *uPort*, *Civic*, e o Projeto *Microsoft* e *Accenture*, com destaque para a Estônia, onde o cidadão tem identidade digital para interação com a maioria dos serviços públicos (SATER, 2017).

É claro que os IDs digitais serão usados em toda a sociedade daqui para frente. Um movimento em direção à auto soberania, identificações digitais combinadas com contratos inteligentes permitiria a maximização total dos direitos do titular dos dados sob o RGPD. Os problemas técnicos atuais na identificação de indivíduos estão sujeitos a processos KYC caros e demorados; dependem de terceiros para armazenamento de dados; e estão sujeitos a alta responsabilidade de salvaguardar os dados pessoais do titular, uma vez que apresenta um claro único ponto de falha e, portanto, um alvo para atores mal-intencionados. Com a identidade controlada pelo titular dos dados, o titular controla seus dados e as contrapartes das transações não retêm dados confidenciais para verificar as transações. A mudança reduziria a responsabilidade, permitindo KYC sem atrito (SATER, 2017, p. 30-31, tradução nossa).

Retira-se, assim, do controlador de dados, a autonomia de criar Ids para os titulares de dados, baseando-se na gravação de operações de registro e operações de compartilhamento, cada qual, com sua descrição adequada:

Assim, os registros de dados podem utilizar dois tipos de transação: uma transação de criação e uma transação de transferência. A transação de criação cria o registro dos dados, que pode incluir mecanismos encontrados no RGPD como consentimento afirmativo, limites de propósitos, o pseudônimo identificação do titular dos dados e condições adicionais para a necessidade de consentimento. Uma transação de transferência, juntamente com a transferência dos dados, poderia mostrar quem agora tem acesso aos dados e sob que condições especificadas ou sujeitas às disposições contratuais que cobrem as questões de acesso. Tudo é claro que dentro das transações há *hash* e *timestamped* (SATER, 2017, p. 36, tradução nossa).

Igualmente, a exclusão de dados também é considerada um problema, uma vez que são conjeturadas situações em que os contratos poderiam ser programados para tornar os dados inacessíveis, com a criação da mutabilidade controlada mediante condições pré-programadas. Essa é, aliás, uma alternativa à característica da *Blockchain* de imutabilidade. A utilização de contratos que são “mortos”, e onde os dados permanecem na *Blockchain*, mas não podem mais ser acessados.

A confiabilidade na *Blockchain* como uma plataforma segura e que mais pode contribuir para a adequação aos regulamentos de proteção de dados está na sua estrutura, que permite que a gravação dos dados seja compartilhada com todos os pontos da rede, bem como sua característica de ser uma rede de consenso, não permitindo que os blocos sejam alterados ou excluídos sem que todos os pontos concordem.

Salmensuu (2018, p. 7) estabelece a distinção entre as *Blockchains* entre “*permissionless*” (como a rede *Bitcoin*), “*permissioned*” (as *Blockchains* privadas) e as híbridas (**Figura 22**). O que muda estas estruturas é o mecanismo de consenso. Na *permissionless*, cada node faz parte do processo de validação de uma transação, sendo

que cada node tem direito de ler e gravar a transação, sendo que nas permissionadas apenas um grupo seletivo dos nodos poderá fazer este processo.

Figura 22: Estrutura das redes *Blockchains*

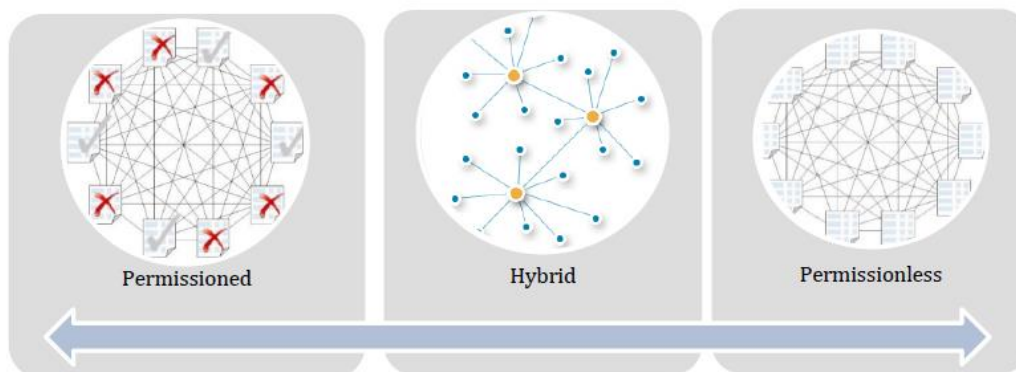
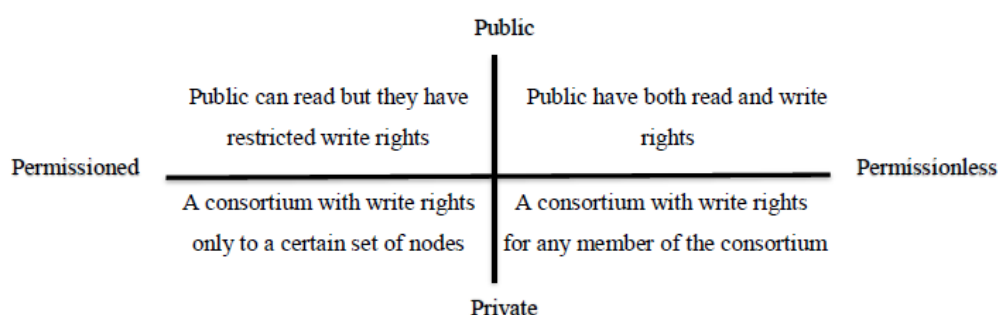


Table 3: *Continuum of blockchains*¹⁵



Fonte: SALMENSUU (2018, p. 7-8)

Ao tratar da encriptação como um dos mecanismos para se guardar dados na *Blockchain*, estabelece que o problema dele é que sempre geram metadados acessíveis por outras plataformas, o que pode constituir em um evidente risco. Quanto à estrutura *Blockchain*, destaca a autora que a *Blockchain* estaria na camada de protocolo e o *bitcoin* estaria na camada de aplicação, assim como o SMTP (*Simplex Mail Transfer Protocol*) está para o *e-mail*.

Estabelece na pesquisa as distinções entre as aplicações permissionadas e não permissionadas na *Blockchain*. Swanson (2015) define que diante da possibilidade de reversibilidade em cadeias não permissionadas o rastreamento de ativos é melhor estabelecido em redes permissionadas. Como estabelece Salmensuu (2018), o gerenciamento de um registro predial, por exemplo, não pode ser revertido, razão pela qual os *Blockchain*

permissionados são os preferidos do setor financeiro, registros de propriedade e de administração tributária, já que resolvem dois males ligados a sistemas centralizados (*falsificação e reversibilidade*) com mais eficiência, somando-se a isto o fato de validar transações por meio de pontos (nodos) que são identificados/conhecidos (diferentemente das *Blockchains* públicas), embora possam estar potencialmente propensos à censura.

Fica evidenciado que os sistemas **centralizados são propensos a exercerem a falsificação e a reversibilidade**. Deste modo, uma controladora de dados pessoais poderia, por exemplo, diante de uma notificação da autoridade de proteção de dados que solicitasse os registros de compartilhamento, “criar” tais registros, ou mesmo “apagar todos os dados”, informando que “nada compartilha”.

Não se tem hoje qualquer garantia a respeito dos registros de compartilhamentos de dados pessoais, importante item para adequação de empresas às regulamentações GDPR e LGPD, já estudadas nesta pesquisa. Salmensuu (2018) também aborda a dificuldade de harmonizar a GDPR com KYC (*Know Your Customer*, Norma anti-lavagem de dinheiro dos Estados Unidos), que exige a identificação de coisas e ativos, mencionando igualmente a reversibilidade das transações poder ser possível, apesar de que existem tecnologias de mistura de dados, como no projeto *Monero*, onde é possível misturar o endereço do gastador com outros endereços, dificultando o rastreamento.

Acerca das limitações do regulamento de proteção de dados em relação à tecnologia *Blockchain*, esclarece que o regulamento não foi concebido para servir um mundo em que os dados são processados sem que alguém os possa identificar. Por outro lado, existe a menção em “Definições” da norma de “sistema descentralizado”, e também trata da questão envolvendo a neutralidade tecnológica, onde se espera que se desconsidere diferenças arquitetônicas no seu processamento (SALMENSUU, 2018, p. 11).

Quanto aos *nodos* – pontos conectados à rede *Blockchain*, conclui que nenhum node se enquadraria como controlador dos dados dentro do contexto da GDPR, considerando que ser controlador pressupõe controle sobre os dados (BERBEICH; STEINER, 2016 *apud* SALMENSUU, 2018, p. 12), entendendo por outro lado que, apesar de entendimentos diversos tornarem uma lacuna sobre a responsabilização, é de se esperar que as autoridades de controle estabeleçam pelo menos algum grau de responsabilização para as empresas que as entidades que adotam estruturas descentralizadas, como avaliação de impacto e controles.

A questão da reversibilidade e da violação à privacidade nas transações na *Blockchain* podem estar ligadas não ao conteúdo em si, que pode ser criptografado ou pseudonimizado, mas aos metadados que são necessariamente gerados na estrutura, por conta do “protocolo de transparência” exigido pela arquitetura, o que pode gerar um risco de identificação (DE FILIPPI, 2016). Conforme o autor, fica muito difícil manter anonimato em uma rede onde o comportamento do usuário é disponibilizado e onde não é necessário sequer muito *expertise* para se reverter e identificar identidades.

De acordo com Sweeney (2002 *apud* SALMENSUU, 2018, p. 18), é possível inclusive identificar dados de saúde relativos a pessoas, correlacionando transações na *Blockchain* com notícias de jornais.

A conclusão é que com a correlação com informações externas é possível associar as chaves públicas entre si, o que pode revelar transações, a exemplo, a pessoa identificada realizou uma transação com o *site* de encontros *online*. Apesar da existência deste risco, o conteúdo dos dados pode ser pseudonimizado ou anonimizado, no primeiro, mantendo-se o controlador de posse de chave de reversão dos dados e, no segundo, desassociando-se de forma definitiva os dados do titular dos dados.

A este respeito, Salmensuu (2018, p. 21) define que é impossível anonimizar os dados completamente de forma irreversível e ao mesmo tempo preservar a capacidade dos nós de compreenderem a transação para executarem o consenso, e neste contexto, os dados da *Blockchain* serão considerados sempre pseudonimizados, sendo estes aqueles em que os dados pessoais não possam mais ser atribuídos a um titular de dados específico sem o uso de informações adicionais, que serão mantidas separadamente, sendo que no conceito da *Working Party 29*, criptografia, funções de *hash* e chave de *tokenização* são consideradas técnicas de pseudonimização.

Outras propostas surgem no sentido de contornar o problema da reversibilidade de dados na *Blockchain*, como a esplanada por Zyskind, Oz e Pentland (2015), que apresenta o registro de dados por meio da combinação de duas cadeias de blocos, sendo uma para acesso e outra com armazenamento de dados, sendo esta mantida por uma *blockchain* permissionada onde apenas o titular dos dados teria acesso. Já a outra cadeia conteria apenas “*hashs*”, logo, não sendo em tese possível identificar o titular dos dados. Por outro lado, sabe-se que *hashs* podem ser considerados dados pessoais.

No que diz respeito aos direitos dos titulares dos dados e o exercício dos mesmos na *Blockchain*, são referenciados o direito a retificação e à exclusão, igualmente como desafios da adoção da tecnologia na harmonização com o regulamento de proteção de

dados pessoais (GDPR). Por outro lado, Salmensuu (2018) estabelece uma alternativa à impossibilidade de exclusão de dados na *Blockchain*, que poderia ser considerada pelas Autoridades de Proteção de dados, sendo esta a limitação do acesso aos dados. “Geralmente, não somos treinados para pensar sobre todas as diferentes maneiras pelas quais a tecnologia pode alcançar os mesmos fins por diferentes meios” (SALMENSUU, 2018, p. 14).

5.1 USO DA *BLOCKCHAIN* E ONTOLOGIAS PARA GESTÃO DO CONSENTIMENTO EM DISPOSITIVOS IoT

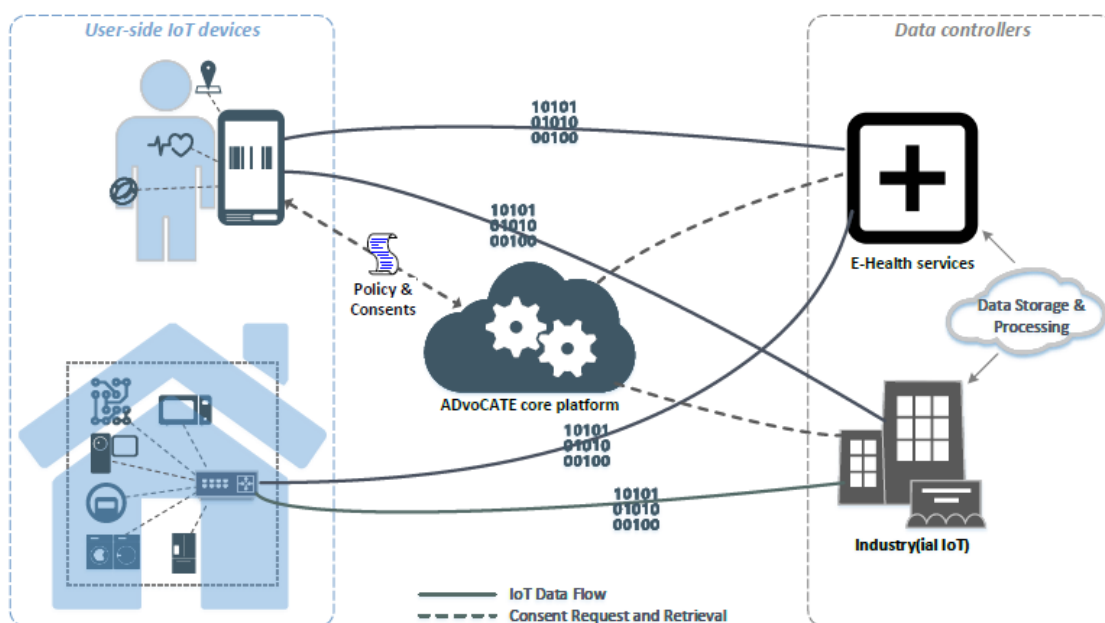
O crescimento dos dispositivos inteligentes constitui uma das grandes ameaças à privacidade e à proteção de dados pessoais. Lucero (2016) estima que teremos 75 bilhões destes dispositivos até 2025 e estes dispositivos poderão monitorar usuários e criar perfis, com ou sem consentimento.

O tratamento de dados de dispositivos IoT comumente é realizado com base no consentimento do titular ou para proteção dos seus interesses vitais. A Lei Geral de Proteção de Dados estabelece que o consentimento deve ser transparente, granular e em linguagem simples e, mesmo quando o consentimento não é requerido, os titulares têm o direito de conhecer os dados pessoais que estão sendo tratados e para quais finalidades.

Cha *et al.* (2018), embora não tratem especificamente de compartilhamento de dados, apresentam uma proposta para que os titulares de dados possam configurar suas preferências de privacidade para dispositivos IoT, interagindo com os mesmos, com a utilização da *Blockchain* para preservar as configurações feitas pelo usuário.

Rantos *et al.* (2018) apresentam o AVOCATE, uma proposta baseada em uma “aplicação central” que faria a intermediação entre os dados coletados por sensores e dispositivos IoT e os controladores de dados, por meio de um sistema de gestão de consentimentos (**Figura 23**).

Figura 23: Infraestrutura do AVOCATE



Fonte: RANTOS *et al.* (2018)

As ontologias são mencionadas como uma forma de resolver os problemas da heterogeneidade dos dispositivos contribuindo para a segurança e privacidade dos usuários (MOZZAQUATTRO *et al.*, 2015 *apud* RANTOS *et al.*, 2018, p. 574), sendo que podem prover uma única descrição para resolver problemas de heterogeneidade no campo da segurança de dados, com regras definidas para o usuário (XU *et al.*, 2017 *apud* RANTOS *et al.*, 2018, p. 574).

No projeto AVOCATE, as ontologias são utilizadas para facilitar as análises das políticas e são baseadas na proposta de Bartolini, Muthuri e Santos (2017), com a descrição de políticas baseadas em linguagens de políticas definidas, como a *eXtensible Access Control Markup Language* (XACML).

Na proposta, os consentimentos são assinaturas digitais gravadas na *Blockchain* e a proposta contempla um único *Smart Contract* entre titular de dados e controlador onde o consentimento é dado e até mesmo removido (momento em que o contrato é atualizado). É criado, também, um mecanismo denominado *consent notary*, que ao final seria responsável por coletar a última versão do *Smart Contract* e gravá-lo na *Blockchain*. Neste contexto é apresentada a solução baseada no usuário para gerenciar seus consentimentos.

O trabalho, no entanto, não trata do registro do compartilhamento de dados pessoais, também não apresentando um padrão de descrição dos dados necessários para

uma política ou contrato eletrônico, mencionando que as ontologias são úteis, o que será desenvolvido em trabalhos futuros.

5.2 UMA PROPOSTA PARA TRANSPARÊNCIA E GESTÃO DE CONSENTIMENTOS

A necessidade de empoderamento do usuário para que este possa rastrear se controladores e processadores acessaram seus dados pessoais vem sendo discutida em trabalhos científicos. Neissel, Steri e Nai-Fovino (2017) estabelecem a proposta de um sistema de transparência e rastreio de proveniência de dados pessoais a partir da *Blockchain*, apresentando dois modelos. O primeiro, onde específicos contratos são gravados na *Blockchain* para cada controlador ou processador recebendo dados pessoais. No segundo modelo, onde cada controlador de dados expressa sua política de uso de dados em um contrato na *Blockchain*, permitindo ao titular dos dados uma interface para entrar e sair do contrato, inclusive revogando o consentimento.

Os pesquisadores avaliam a possibilidade de dois modelos de contrato para registro de dados pessoais, sendo o primeiro baseado no titular dos dados, realizando um contrato para cada um dos controladores de dados; o segundo, onde o titular de dados não realiza um registro ou contrato para cada controlador, mas para o tipo de dados; o terceiro, onde o controlador disponibiliza na *Blockchain* o referido contrato para cada um dos seus clientes, onde os titulares de dados possam ingressar e aceitar os usos e políticas, muito parecido com as políticas de privacidade (NEISSEL; STERI; NAI-FOVINO, 2017).

A proposta apresenta a organização de dados de uma política de privacidade em um contrato inteligente. A questão sobre a privacidade dos registros de contrato também é abordada, considerando que utilização de um endereço único para o titular de dados poderia rapidamente revelar sua conexão com os controladores de dados, o que pode expor para demais pontos que vejam uma rede pública as suas preferências e hábitos (NEISSEL; STERI; NAI-FOVINO, 2017, p. 5).

A rastreabilidade de dados pessoais poderá, a partir da organização em contratos, permitir que o titular dos dados, por exemplo, questione alguém que lhe envia mensagens a seu *e-mail* pessoal, ao qual não possuiu qualquer relação prévia, o que contribuiria inclusive para auditoria a ser realizada pelas Autoridades de Supervisão e Proteção de Dados Pessoais.

A sinalização de atividades não conformes pode desencadear uma investigação e auditoria na organização pelo Conselho Fiscal Autoridades e possivelmente levar a uma sanção caso a organização não possa informar as respectivas transações no *blockchain*, permitindo que os dados sejam recebidos e usados para o propósito específico (NEISSEL; STERI; NAI-FOVINO, 2017, p. 6, tradução nossa).

Neste contexto, alguém que receba um anúncio, por *e-mail*, por exemplo contendo dados pessoais, sem que conheça a fonte, pode constituir um indicativo de compartilhamento de dados em desconformidade. Nos contratos com base no titular de dados, quando este cadastra-se no serviço do controlador, é criada uma política baseada no uso de dados, especificando restrições no uso e redistribuição de qualquer dado obtido implícita e explicitamente pelo controlador envolvendo:

Dados explícitos são quaisquer dados submetidos diretamente pela interação entre o titular dos dados e controlador, sendo que este detém a consciência dos dados que estão sendo fornecidos.

Dados implícitos são dados coletados automaticamente, como por exemplo, dados de sensores de equipamentos IoT, dados de aplicativos e dispositivos móveis, ou mesmos dados e *logs* de servidores que podem registrar as interações na rede, incluindo endereços IP (*Internet Protocol*) (Figura 24).

Figura 24: Arquitetura do *Subject Contract Model*

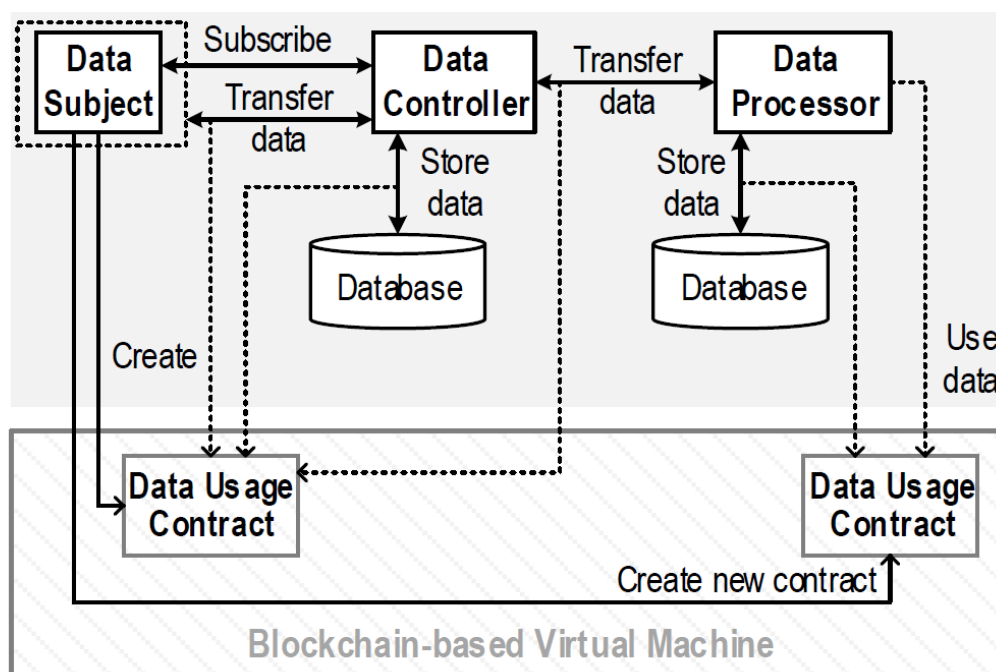


Figure 1: Architecture

Fonte: NEISSEL; STERI; NAI-FOVINO (2017, p. 6)

Como se verifica, não só para cessão de dados pessoais ao próprio controlador, mas em cada transferência de dados do controlador para o processador de dados, novos contratos seriam criados cientificando o titular dos dados, que pode recusar qualquer operação (Figura 25).

Figura 25: Diagrama do *Subject Contract Model*

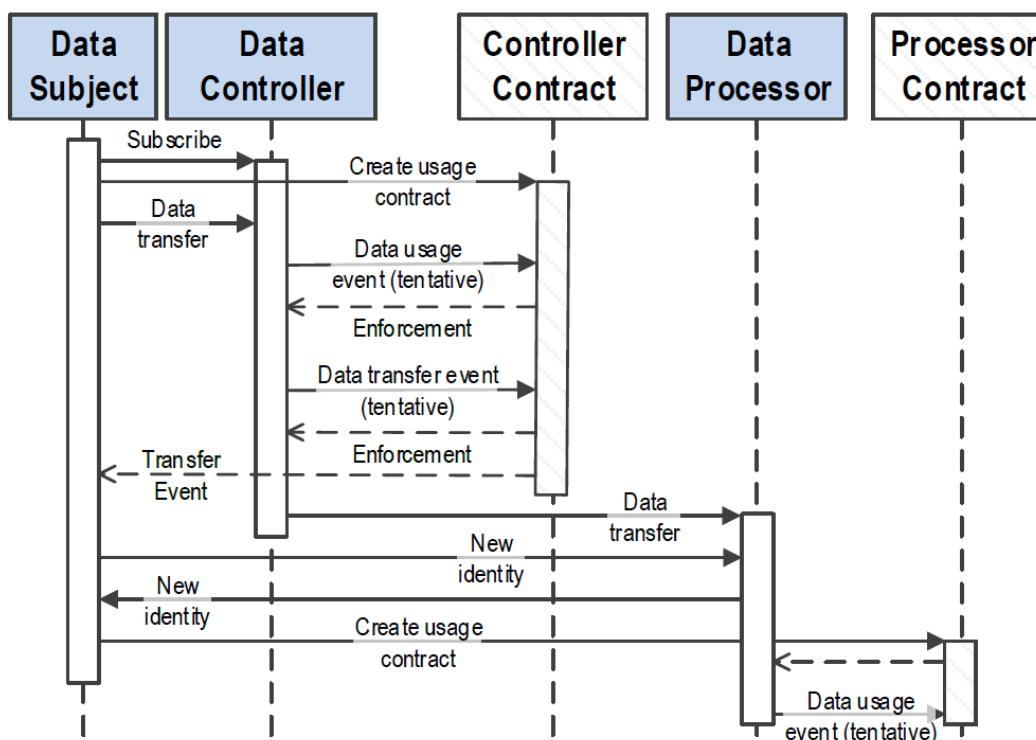


Figure 2: Sequence diagram

Fonte: NEISSEL; STERI; NAI-FOVINO (2017, p. 6)

Pela estrutura, o titular dos dados realiza a subscrição do serviço e neste momento o controlador de dados ativa o contrato na *Blockchain*, que traz informações sobre o uso de dados, possível transparência de dados, sendo que com a aceitação os dados são transferidos.

Com a condição de possibilidade de transferência aceita, habilita-se ao controlador transferir os dados para o processador. Neste momento o controlador pode transferir dados a terceiros, sem que tal transferência gere um registro para o titular. Quando o controlador transfere os dados, ele envia a identidade do processador que só o titular vê, então, o titular estabelece um novo contrato com o processador. A exclusão de permissão de tratamento se daria com a exclusão do contrato da *blockchain*, o que

manteria o contrato inativo para aquele momento, preservando-se o histórico do contrato (NEISSEL; STERI; NAI-FOVINO, 2017, p. 6).

As políticas são parametrizadas e programadas em contratos eletrônicos e poderiam disciplinar todos os usos dos dados, com os quais poderá o titular concordar ou não (**Quadro 12**):

Quadro 12: Política para envio de e-mails a cada 30 dias e configurações de Política para compartilhamento de dados com a finalidade de marketing do país “Itália”

Código	Explicação da política
Default Enforcement: Deny PolicyTemplate0 Variables: Entity(s) Event: sendMessage(purpose= billing , isDataSubject(e-mail, s)) Condition: not(within(30 days, sendMessage(purpose= billing , isDataSubject(e-mail, s)))) Action: Allow ConfigurationTemplate0 Variables: Entity(s) Assignments: s = xpath(\\trigger\\user) Event: subscribeUser() Condition: true Action: configure(PolicyTemplate0, s) PolicyTemplate1 Variables: Entity(s) Event: shareData(purpose= marketing , country= Italy , isDataSubject(country, s)) Condition: true Action: Allow	Padrão de consentimento negado Primeira Política Criação de uma Entidade de Política Definição do evento para envio de Mensagem a cada 30 dias Definição da condição Titular dos dados Aceitação da Política Configurações da Política Varável entidade Assinaturas Dispara o evento assinatura do usuário Condição Ação para a Primeira Política Segunda Política Criação de uma entidade de Política Definição de compartilhamento de dados Titulares de dados do país Condição verdadeira Aceitação da Política

Fonte: adaptado pelo autor de NEISSEL; STERI; NAI-FOVINO (2017, p. 9)

Pelo que foi identificado, esta é uma proposta de contrato inteligente autoexecutável. Não foi identificada uma padronização para contratos inteligentes de transferências de dados. No exemplo citado por Neissel, Steri e Nai-Fovino (2017), adição de metadados sob as condições como os tipos de dados e talvez descrição mais precisa sobre os dados, poderiam contribuir para maior organização das informações sobre as condições de compartilhamento. Do mesmo modo, as permissões adicionais podem ser interessantes para um consentimento granular, que é exigido pelas Leis de Proteção de Dados.

5.3 A *BLOCKCHAIN* COMO MECANISMO DE GARANTIA DE DIREITOS E OS REGISTROS IMUTÁVEIS

A *Blockchain* vem sendo considerada em pesquisas recentes como um recurso para assegurar os direitos trazidos pelos regulamentos de proteção de dados. Em essência é caracterizada por um livro razão contendo linhas de dados ou informações. A rede é considerada distribuída e quando um bloco é acrescentado na mesma e cada nó recebe também a referida informação, o que gera confiabilidade.

Enquanto em uma rede tradicional o titular dos dados precisa acreditar na confiabilidade de cada ponto da rede, como no aplicativo de internet *banking*, que usa um servidor central para autenticar o usuário, a *Blockchain* não exige que os usuários que participam dela tenham confiança entre si, graças a sua característica de ser uma *distributed ledger technology* (DLT), significando que se um node alterar um dado pré-existente ele é rejeitado pelos demais nodos, assegurando integridade dos registros, logo um registro adicionado no livro razão é indelével.

Neste ponto, um aparente conflito existiria entre os regulamentos de proteção de dados e a característica da *Blockchain*: Se os registros são indelévels, como o titular de dados poderá assegurar e exercer um de seus direitos previstos na LGPD e GPDR, a exclusão dos dados pessoais que não são mais necessários, ou mesmo alterar dados inexatos. Neste ponto, outras pesquisas trazem novos endereçamentos ao tema.

A *Blockchain* pode se caracterizar por ser pública ou privada. A pública se define como aquela em que todos os participantes ou nodos tem direitos iguais e não existe um grupo fazendo a governança. Já uma *Blockchain* privada pode se caracterizar por aquela onde se pode definir: a) quem são o nodos; b) quem pode acessá-la; c) quais informações podem ser visualizadas; e d) quem pode vê-lo.

A *Blockchain* opaca ou privada torna possível e seguro processar dados pessoais em conformidade com a GDPR (HEUKELOM; NAVES; VAN GRAANFEILAND, 2017).

Geelkerken e Konings (2017) enfrentam o tema, direcionando que alternativas para o apagamento seria a criptografia dos dados pessoais com a exclusão da chave depois, de maneira que os originais não seriam apagados, mas um bloco adicional seria adicionado detalhando a criptografia. Já no que diz respeito a alteração de dados, poderia ser resolvido com a adição de um bloco com a informação atualizada.

Por outro lado, não se pode garantir que o controlador não tenha realizado cópias dos dados descobertos antes de criptografia e gravação na *blockchain*. Este é um ponto crítico envolvendo a *Blockchain* pública, além da necessidade de ter que realizar inúmeros contratos de processamento de dados pessoais pelos nodos da rede, que seriam considerados processadores, o que torna o processamento inviável.

A situação é diferente quando se trata de uma *Blockchain* privada. Considerando que nesta alguém pode deter o controle de 50% + 1 de todos os nós ou outra forma de governança da rede, considerando que a remoção ou o apagamento dos dados poderia ser feito com a maioria dos nós apagando os dados e posteriormente o restante repetindo o procedimento, o mesmo ocorrendo para solicitação de alterações de dados. (GEELKERKEN; KONINGS, 2017).

A pesquisa, no entanto, não trata do registro do compartilhamento de dados, do mesmo modo, não prevendo o padrão de descrição dos dados, ou como seriam organizados para que possam ser gravados na *Blockchain*. Oferece, no entanto, importante contribuição no sentido de expor os riscos das *Blockchains* públicas no que tange à alteração e exclusão de dados e a proposta com base em *Blockchains* privadas.

5.4 A *BLOCKCHAIN* PARA REGISTRO DE AUTORIZAÇÕES E *LOGGING* DAS ATIVIDADES

A *General Datas Protection Regulation* trouxe de volta aos titulares de dados o controle sobre tais dados pessoais, trazendo importantes obrigações aos agentes de tratamento. Revela-se de muita importância o titular dos dados poder supervisionar se efetivamente um agente de tratamento está em conformidade ou não com a norma. Neste contexto, a *Blockchain* tem potencial para servir de plataforma para que o agente de tratamento e titular de dados possam realizar o intercâmbio de dados pessoais, por meio de *smart contracts*, registrados de forma indelével na *blockchain*, gerando-se *logs* de todas as atividades realizadas.

Apesar dos regulamentos trazerem a necessidade de conformidade, existem lacunas graves de transparência e é praticamente intangível que um agente de tratamento demonstre transparência e conformidade utilizando soluções centralizadas.

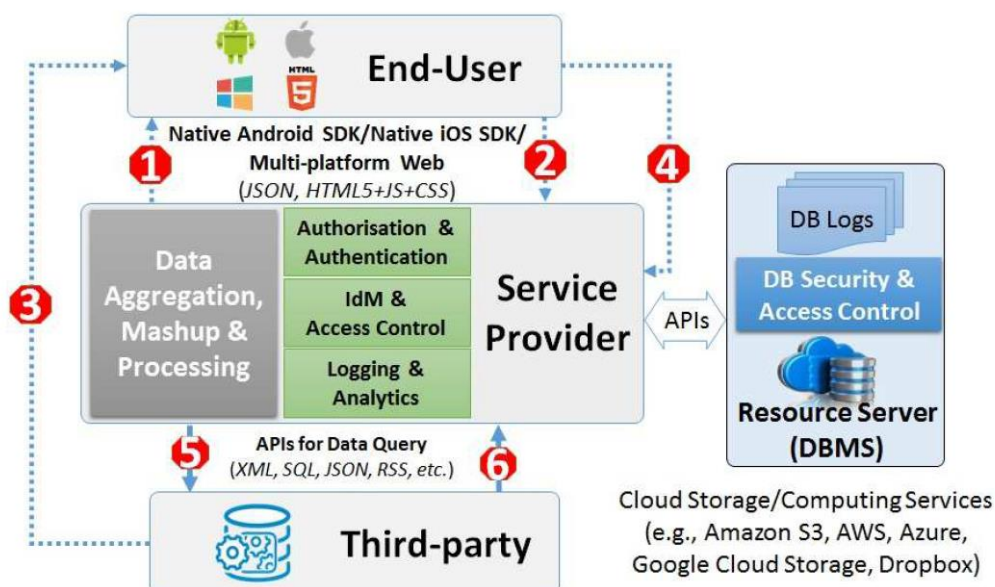
A tecnologia *Blockchain* pode ser concebida como um conjunto de técnicas diversificadas, incluindo sistemas distribuídos, redes de computadores, bancos de dados e criptografia, desenvolvendo um papel de um livro razão distribuído. A *Blockchain* pode

atuar na concepção de *smart contracts*, promovendo importantes contribuições no que diz respeito a este desafio, trazendo descentralização, resistência ao tempo, transparência e rastreabilidade. Um *smart contract* é um programa de computador desenvolvido sobre a rede *Blockchain*, sendo que automaticamente executa ações a partir de condições pré-programadas (TRUONG *et al.*, 2019).

Os sistemas oferecidos pelos agentes de tratamento de dados a titulares para fornecimento ou coleta de dados possuem estruturas proprietárias, centralizadas, onde fica dificultoso identificar o que realmente é feito com os dados pessoais “intramuros”. Truong *et al.* (2019) detalham o modelo atual de transação de dados entre titulares e agentes, apresentando importantes desafios e nítidas opacidades para o dono dos dados.

Normalmente os titulares de dados iniciam o serviço de um agente de tratamento, que pede permissão para acesso a seus dados pessoais, o usuário então concede tais permissões, um agente terceiro indaga o titular de dados para tratar seus dados, que são coletados e gerenciados pelo agente de tratamento. Quando o titular dos dados se conecta ao serviço, ele concede um conjunto de permissões para terceiros. Quando esta permissão é garantida, o agente de tratamento autoriza o terceiro a tratar os referidos dados e então este terceiro (processador), aciona uma API, usando um *token* oferecido, para ter acesso aos referidos dados (TRUONG *et al.*, 2019, p. 4) (**Figura 26**).

Figura 26: Esquema pessoal de gestão e compartilhamento de dados em uma arquitetura-cliente servidor



Fonte: TRUONG *et al.* (2019, p. 5)

Nesta perspectiva, como identificado na pesquisa analisada, o titular dos dados os fornece com base em um único mecanismo de autenticação a utilização de dados pessoais por terceiros. Os registros das atividades (*logs*) são vistos apenas pelo Agente de tratamento (*service provider*, SP). Do mesmo modo, as requisições de dados feitas por terceiros (*third-party*, TP) são realizadas via APIs, códigos de transferência de dados, sem que o titular dos dados tenha acesso. Este modo não permite que um Agente de tratamento de dados pessoais comprove que está processando de forma regular e segura dados pessoais. Do mesmo modo, o usuário não tem transparência sobre as operações de tratamento após fornecer os dados, o que pode gerar riscos.

Da perspectiva do usuário final, isso leva à falta de transparência e responsabilidade do gerenciamento de dados e aumentar riscos de vazamento de dados pessoais. Como todos os mecanismos de gerenciamento de dados são operados em um sistema centralizado e sob o controle, o SP ainda poderá entregar dados pessoais a um TP não autorizado sem o conhecimento do usuário final, como na medida em que não seja investigado pelas autoridades de supervisão. Do ponto de vista de um SP, como a investigação da autoridade supervisora é ocasionalmente realizada, é um desafio para um SP declarar que está processando de forma contínua, segura e legal todos os dados pessoais, conforme necessário (TRUONG *et al.*, 2019, p. 4, tradução nossa).

Os autores propõem um modelo conceitual para uma plataforma de gestão de dados pessoais em conformidade com a GDPR (norma Europeia), onde basicamente as autorizações, consentimentos relativos ao tratamento de dados pessoais e os *logs* não ficam especificamente na plataforma do agente de tratamento, mas sim registrados em um *smart contract* que utiliza de base a plataforma *Blockchain*. A *Blockchain* armazenaria um *token*, como “prova de permissão”, assegurando à parte interessada a comprovação de que obteve acesso a dados pessoais (**Figura 27**).

Figura 27: Design de modelo de gestão de dados pessoais baseados na *Blockchain*

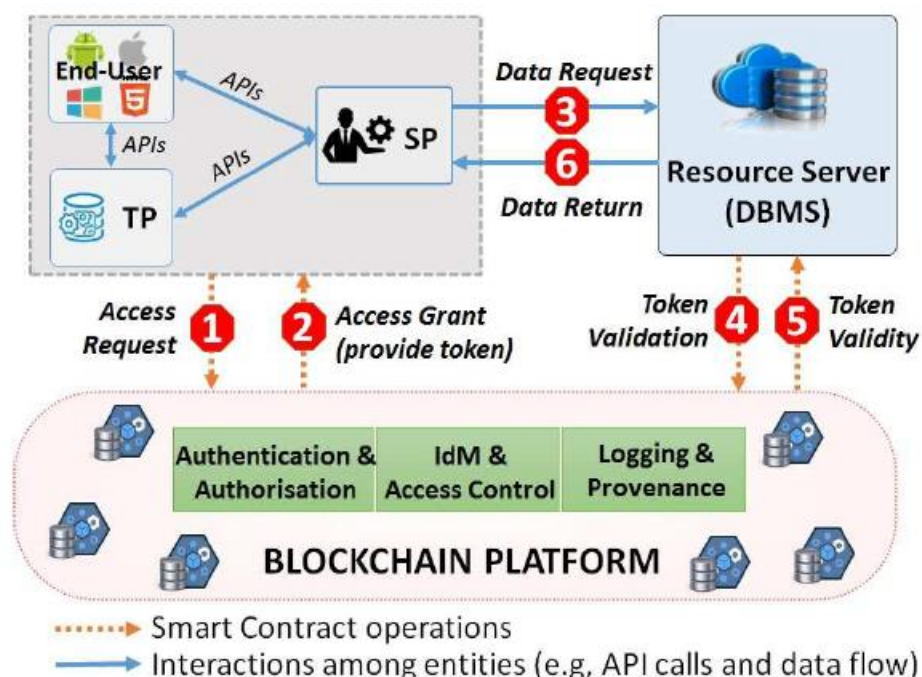


Fig. 2: High-level system architecture of the design concept for a BC-based personal data management platform. The operation flow consists of 6 steps, among which step 1, 2, 4, and 5 are dedicated to granting and validating permissions operated through Smart Contracts. Step 3 and 6 operated via API calls and data-flow from/to an Resource Server.

Fonte: TRUONG *et al.* (2019, p. 5)

No modelo proposto, as requisições de dados entre titular e agente de tratamento (controlador) e agente de tratamento (processador) ou terceiro são feitas via API e, necessariamente, precedem uma requisição de acesso ao *Smart Contract*, que armazenaria o “*token*” do titular como “prova de autorização”. Quando o acesso é dado, o *Smart Contract* devolve a informação ao agente de tratamento que solicitou, o que inicia uma requisição na base de dados. Antes, porém, de os dados serem retornados, o *Token* do titular dos dados é validado novamente no *Smart Contract* e, com a validação, os dados são retornados, sendo que a transação fica registrada através da funcionalidade de “*logging & provenance*”.

A proposta considera o registro de par de chaves e um “*state*” (*status*) com um registro no *ledger* (*Blockchain*), podendo ser a criação, atualização ou exclusão de um par de chaves (**Quadro 13**). O *ledger* registra todo o histórico das transições de “*state*” com o registro do tempo, na ordem mais recente de adição do bloco.

Quadro 13: “A ledger” utilizado para autenticação, autorização e acesso

<p><i>Listing 1: A state of the 3A ledger in JSON format. Content of the ledger includes en pointer: ciphertext of a data pointer; pk enc: public key used to encrypt the en pointer; policy: data usage policy, and hash of the data.</i></p>	
<pre> 1 {"3A_ledger": { 2 "key": { 3 "owner": pk_DS, 4 "controller": pk_DC 5 } 6 "value" { 7 "en_pointer": 8 3erwf3ese6d5c4..., 9 "policy": { 10 "rule": 11 {Effect},{Condition}, 12 "action": "read, 13 update", 14 "target": "{pk_1, pk_2, 15 ...}" 16 }, 17 "pk_enc": 18 "fMA0GCSqGSib3...", 19 "hash": 20 "369f2e3e69dc40543...", 21 "timestamp": 22 1549480378 23 }} </pre>	<p>1 Nome do livro razão 2 Função que armazena as chaves 3 Chave do titular de dados pessoais 4 Chave do controlador de dados 6 Armazena dados relativos ao gerenciamento de dados 7 Conteúdo criptografado do ponteiro de dados 8 Política de uso dos dados pessoais 9 Regras e condições 10 Permissões inerentes a coleta de dados 13 Chave utilizada para criptografar o ponteiro de dados 14 Hash dos dados 15 Carimbo do tempo</p>

Fonte: adaptado pelo autor de TRUONG *et al.* (2019, p. 7)

Como se pode verificar, os autores descrevem em linguagem estruturada um “registro” a ser adicionado no livro razão *Blockchain*, a partir de um *Smart contract*, que permitiria assegurar, em tese, a “autenticidade de autorizações e consentimentos” para uso de dados pessoais. Os autores também descrevem a estrutura de dados para o livro de “logs”, diversa do livro “A ledger” acima citado, e que registraria todas as autorizações e revogações realizadas.

Deste modo, trata-se de uma proposta em que se pode identificar características no que tange à organização da informação:

- a) Remove do controlador dos dados a guarda exclusiva dos registros de autorização e logs das atividades;
- b) É baseado em uma linguagem de descrição organizada (JSON, *JavaScript Object Notation*);

- c) Considera um *Smart contract*, linguagem computacional, com capacidade de interagir na *Blockchain*;
- d) Criptografa o *set* de dados, evitando que seja analisado por outras pessoas.

A linguagem adotada para descrição dos dados gravados na *ledger* denota uma importante tendência. A necessidade de um padrão para descrição dos dados. Neste sentido, para que dados sejam legíveis por máquinas é possível utilizar o formato de serialização como JSON (MELHORES PRÁTICAS PARA DADOS NA WEB, 2016).

No entanto, o sistema proposto pelos autores:

- a) Está relacionado a uma gestão de compartilhamento de dados onde todo o tratamento necessitaria uma requisição de acesso. Ocorre que os processadores ou terceiros que tratam dados pessoais em muitas situações não possuem contato direto com o titular dos dados, razão pela qual não realizam “requisições de acesso”;
- b) Assim, o registro de uma autorização de acesso seria feito para o “controlador”, que pode registrar no contrato eletrônico a permissão de compartilhamento; no entanto, isto equivale às políticas de privacidade atuais. O titular continuará sem saber os fluxos dos seus dados e para quais processadores migraram os referidos dados;
- c) Do mesmo modo, considera-se dados organizados e coletados pelo próprio *Smart Contract* para ser gravado na *Blockchain*, no entanto, não apresentam no modelo metadados (dados sobre dados) que seriam essenciais que fossem compartilhados, como “a categoria dos dados” e o “tipo de coleta”, “*dataset* enviado” informações que proporcionariam transparência ao titular dos dados;
- d) Os *datasets* de informação são encaminhados à *Blockchain*, o que pode constituir, em *blockchains* públicas, um risco à segurança da informação.

Informações capturadas ou geradas de recursos informacionais podem ser úteis no entendimento sobre a que se referem. Estas informações podem ser lidas por máquinas e podem ser usadas para descrever um recurso, como uma transferência de *datasets* de dados pessoais, rotulando-a a partir de sua análise. Assim como os dados descritivos de um livro, os metadados podem ser utilizados para descrever características de um *dataset* e, a partir deles, o registro das transações poderá conter informações que irão proporcionar

maior transparência ao titular dos dados (LIMA; SANTOS; SANTARÉM SEGUNDO, 2016).

Pode-se definir metadados como “dados ou informações que permitem às pessoas exercerem determinadas funções em relação aos recursos de informação a que os metadados se referem [...]” (MILLER, 2004, p. 1, tradução nossa).

A *National Information Standards Organization*, no documento “*Understanding Metadata*” descreve metadados como a informação estruturada que descreve, explica, localiza ou possibilita a fácil recuperação de um recurso informacional (NISO, 2017). Neste sentido, apresenta-se nesta presente pesquisa uma proposta de modelo conceitual de estruturação de informações sobre transferência de dados, de uso de sistemas computacionais para registro na *Blockchain*.

Fornecer informação descritiva sobre os *datasets* a serem compartilhados permite que os *user agents* descubram automaticamente os *datasets* disponíveis na *Web*, além de permitir aos humanos entender a natureza do *dataset* e suas distribuições (MELHORES PRÁTICAS PARA DADOS NA WEB, 2016).

5.5 REQUISITOS E SISTEMAS PARA REGISTRO TRANSPARENTE DE LOGS DE ATIVIDADES ENVOLVENDO COMPARTILHAMENTO DE DADOS PESSOAIS

Discussão sobre meios válidos para registros das atividades envolvendo dados pessoais é apresentada por Piero Bonatti *et al.*, 2020, que partem do princípio de que os *logs* são atividades centrais e essenciais para assegurar a transparência aos titulares de dados. Os autores apresentam os mecanismos identificados com válidos para *logging* (registro) de atividades, a possibilidade de serem auditados e desafios.

Para que empresas demonstrem sua adequação às leis no que diz respeito ao tratamento de dados pessoais, o primeiro passo é a criação de um registro (*ledger*), de todas as transações, capaz de demonstrar o que acontece com os dados. Neste sentido para que este registro seja efetivo, ele deverá considerar: a) funcionalidades; e b) elementos robustez, a seguir apresentadas no **Quadro 14**:

Quadro 14: Funcionalidades e elementos de funcionalidade de registros de atividades com dados pessoais

Elemento	Motivo
Compleitude	Todos os eventos de processamento e compartilhamento de dados devem ser registrados no livro-razão.
Confidencialidade	Tanto os titulares dos dados quanto as empresas só devem ser capazes de ver as transações que envolvem seus próprios dados.
Exatidão	Os registros armazenados no livro-razão devem refletir com precisão o processamento evento.
Imutabilidade	O <i>log</i> deve ser imutável de forma que não seja possível rastrear e reinventar a história.
Integridade	O <i>log</i> deve ser protegido de modificações acidentais e/ou maliciosas.
Interoperabilidade	A infraestrutura deve ser capaz de transcender os limites da empresa controladora, no sentido de que o titular dos dados deve ser capaz de combinar facilmente os registros que obtém de várias empresas.
Não repúdio	Quando se trata de processamento de dados e compartilhamento de eventos, não deve ser possível negar posteriormente que o evento ocorreu.
Retificação & Apagamento	Deve ser possível retificar erros nos dados pessoais armazenados e/ou excluir dados a pedido do titular dos dados.
Rastreabilidade	Em caso de processamento deve ser possível saber sobre qualquer processamento anterior dos dados. Como tal, deve ser possível vincular eventos de uma maneira que suporte a rastreabilidade do processamento.

Fonte: adaptado pelo autor de BONATI *et al.*, 2020, tradução nossa

Do mesmo modo, apresenta a robustez que o sistema de registros deverá conter, incluindo a disponibilidade, performance, escalabilidade. Além disso, sobre o armazenamento, importante destacar que boa prática é reduzir a quantidade de informações armazenadas no *log*, e os próprios dados devem ser armazenados em outro lugar e apenas um *hash* dos dados e um ponteiro para os próprios dados reais devem ser armazenados no livro razão (BONATTI *et al.*, 2020, p. 4).

Partindo das funcionalidades e dos elementos de robustez, os autores avaliam três (3) soluções candidatas a registradores transparentes de atividades de tratamento ou operações de dados pessoais:

- a) **Registros locais:** cada ponto pode armazenar os registros de *logs* localmente, utilizando-se de recursos de segurança para garantir a integridade dos *logs*, como a assinatura de chave secreta e códigos de autenticação de mensagem (MACS), garantindo-se que entradas anteriores de *logs* não podem ser modificadas (BONATTI *et al.*, 2020, p. 5);

- b) **Terceiros confiáveis:** outra alternativa é confiar o registro de *logs* aos denominados *Trusted Third Party* (TTPS), também mantendo técnicas de registro seguro (MACS). Um agente terceiro de confiança seria responsável por gerar o código de autenticação por mensagem (MAC), criptografado com a chave pública do usuário, assinando-o com sua própria chave privada e remetendo ao titular dos dados. No caso de compartilhamentos dos dados, uma nova chave pública é criada de modo que a chave privada do titular possa descriptografar (BONATTI *et al.*, 2020 p. 5);
- c) **Registros globais ponto a ponto:** aqui o *ledger* (registro) seria distribuído por diversos registradores físicos, se tornando um registrador virtual global. Neste aspecto a *Blockchain* pode ser útil, onde os dados seriam criptografados com uso de uma chave conhecida pelo controlador e titular e seriam enviados à *Blockchain* de forma cifrada e sem a chave, com um ponteiro para os dados na *blockchain* na forma de um *hash*. Assim, identidades garantiriam que apenas usuário e controladores conseguiriam descriptografar os dados. Como desafios, no entanto, registram que, ao contrário de terceiros confiáveis, as *Blockchains* não tem acordos de nível de serviço, o que pode comprometer o elemento “disponibilidade”.

Quando à terceira modalidade, concluem que ainda não foram utilizadas:

Em comparação com as abordagens locais ou globais que empregam terceiros, a robustez das abordagens propostas não foi explorada até o momento, e é difícil de avaliar a eficácia dos registros P2P ou *blockchains* de uma perspectiva não funcional (BONATTI *et al.*, 2020, p. 7, tradução nossa).

Para descrição dos dados, o *Resource Description Framework* (RDF), fundamental no *LinkedDataWeb* (LDW), é caracterizado como meio de representar e vincular informações de uma maneira que possam ser interpretadas por humanos e máquina, tendo sua utilidade na descrição por metadados dos registros de compartilhamento de dados.

Ao empregar técnicas de RDF para representar os eventos de proveniência armazenados no livro-razão, seremos capazes de oferecer suporte não apenas à interoperabilidade entre os livros-razão, mas também à rastreabilidade entre os eventos em um manual que facilita a verificação automática de conformidade. (BONATTI *et al.*, 2020, p. 7, tradução nossa).

Os autores apresentam a possibilidade do uso de ontologias como PROV5 e OWL-Time6 que poderiam ser úteis na descrição dos registros envolvendo o compartilhamento de dados pessoais.

5.6 DISCUSSÃO SOBRE PONTOS OBSERVADOS NAS PESQUISAS SOBRE USO DA *BLOCKCHAIN* NO REGISTRO DE ATIVIDADES

Nas pesquisas realizadas sobre a *Blockchain* e proteção de dados, identificou-se grande desafio existente no exercício dos direitos de apagamento e retificação (FABIANO, 2018). Do mesmo modo, a questão da privacidade dos dados em tecnologias descentralizadas é tratada como um desafio dos regulamentos no entendimento da estrutura descentralizada (EICHLER *et al.*, 2018).

Para o contorno dos riscos envolvendo violações à privacidade na *Blockchain* está a possibilidade de *hashing* do *dataset* de maneira que os dados não possam ser reconstruídos (EICHLER *et al.*, 2018). Por outro lado, conforme mencionado anteriormente, para Filipponi (2017) a *Blockchain* pode gerar aos indivíduos mais privacidade e autonomia do que em sistemas centralizados, apresentando o papel trágico da centralização, que não favorece o controle dos titulares em relação a seus dados pessoais, priorizando a transparência.

Do mesmo modo, as pesquisas indicam riscos de soluções com base em *Blockchains* públicas, que poderiam estar sujeitas à centralização e dar origem a novas formas não oficiais de controlar o sistema (FILIPPONE, 2017). O risco de reversibilidade dos dados em cadeias não permissionadas é destacado por Swanson (2015).

Para registros que não podem ser revertidos são usados, preferencialmente, os *Blockchain* permissionados, por gerenciarem melhor questões relacionadas à falsificação e reversibilidade, além de usar nodos para validar as transações (SALMENSUU, 2018). **Estes são os sistemas identificados nas 5 (cinco) aplicações analisadas nesta pesquisa.**

Como alternativa às características da *Blockchain* que impedem a exclusão de dados, Salmensuu (2018) estabelece importante solução de contorno, a limitação de acesso aos dados gravados na *Blockchain*. Geelkerken e Konings (2017) também enfrentam o tema, direcionando que alternativas para o apagamento seria a criptografia dos dados pessoais com a exclusão da chave depois, de maneira que os originais não seriam apagados, mas um bloco adicional seria adicionado detalhando a criptografia. Já

no que diz respeito à alteração de dados, poderia ser resolvido com a adição de um bloco com a informação atualizada.

Já Sater (2017) discorre sobre a criação de um consórcio *Blockchain* que, uma vez alinhado com o cenário regulatório, permitiria a troca de dados entre empresas do mundo todo, com a garantia de assegurar que os usuários possam rastrear seus dados por meio de IDs digitais. O autor ainda discorre que o uso de IDs digitais pelos titulares dos dados permite maior controle do uso dos dados, uma vez que dados confidenciais não serão retidos para verificação das transações realizadas.

Retira-se, assim, o poder dos controladores de dados em criarem IDs para os titulares de dados pessoais, o que é muito comum nas aplicações atualmente. Do mesmo modo, os registros de transferência poderiam mostrar quem tem acesso aos dados e sob que condições, dentro de transações com *hash* e carimbo do tempo (SATER, 2017).

De fato, em se tratando de *Blockchains* privadas e em se considerando que são conhecidos todos os nós (nodos) que farão o consenso de uma transação, seria possível alterarmos e excluirmos dados da *blockchain*, desde que a maioria dos nós (nodos) apagasse os dados (GEELKERKEN; KONINGS, 2017).

Resta evidente, assim, que as *Blockchains* privadas ou permissionadas oferecem maior privacidade em projetos que pretendam registrar a transferência de dados pessoais.

Neissel, Steri e Nai-Fovino (2017) estabelecem a possibilidade de políticas de privacidade interativas, com base em contratos inteligentes (*Smart Contracts*), descritos na *Blockchain*.

Como se constatou, os sistemas oferecidos pelos agentes de tratamento de dados a titulares para fornecimento ou coleta de dados possuem estruturas proprietárias, centralizadas, onde fica dificultoso identificar o que realmente é feito com os dados pessoais, não só na fase de coleta, mas principalmente, em relação às operações de compartilhamento. **Conforme verificado no trabalho de Truong et al. (2019), da perspectiva do usuário final, isso leva à falta de transparência e responsabilidade do gerenciamento de dados e aumentam riscos de vazamento de dados pessoais.** Como todos os mecanismos de gerenciamento de dados são operados em um sistema centralizado e sob o controle, o controlador ainda poderá entregar dados pessoais a um terceiro não autorizado sem o conhecimento do usuário final, na medida em que não seja investigado pelas autoridades de supervisão.

A proposta dos autores citados também considera um contrato inteligente, em que é atualizado seu “*state*” a cada transferência de dados. De forma a considerar a limitação

da não exclusão de dados pessoais na *Blockchain*, o “*state*” do contrato poderia ser atualizado de uma forma que impedisse que pessoas tivessem acesso ao contrato. Por fim, RANTOS *et al.* (2018) apresentam o AVOCATE, uma proposta baseada em uma “aplicação central” que faria a intermediação entre os dados coletados por sensores e dispositivos IoT e os controladores de dados, por meio de um sistema de gestão de consentimentos baseado na *Blockchain*. Os autores também mencionam que as ontologias podem resolver os problemas da heterogeneidade dos dispositivos, e contribuir para a segurança e privacidade dos usuários sem, contudo, exemplificarem.

Deste modo, revisada a literatura que trata de *Blockchain* para registro das atividades, identificam-se algumas premissas no que tange à organização da informação sobre usos e compartilhamento de dados pessoais. As aplicações que surjam com esta finalidade devem:

- a) **Remover do controlador dos dados** a guarda exclusiva dos registros de autorização e *logs* das atividades;
- b) **Ser baseado em uma linguagem de descrição organizada**, para se evitar desconformidades, podendo-se contar com o uso das ontologias; esta linguagem descreverá campos, finalidade, tipo de dados, dados de quem receberá os dados e demais informações;
- c) **Utilizar técnicas para evitar violação dos direitos dos titulares como a impossibilidade de exclusão ou retificação de dados**, podendo ser, como visto, proibição de acesso a dados, *hash* dos *datasets*, armazenamento de dados fora da *blockchain*, alteração do “*status*” de um contrato inteligente, e uso de *Blockchains* não permissionadas ou privadas, onde pode-se exercer uma governança incluindo a possibilidade de exclusão dos referidos dados.

Como verificado, apesar de a *Blockchain* apresentar características e princípio conflitantes, como a latente questão da impossibilidade de exclusão dos dados registrados na cadeia de blocos (FABIANO, 2018), identificou-se na pesquisa que já se discute soluções de contorno, que possibilitem o uso da tecnologia, com propostas científicas como a limitação do acesso aos dados gravados na *Blockchain* (SALMENSUU, 2018), a adição de *Blockchains* permissionadas (SWANSON, 2015), a geração de *hashing* dos *datasets* e não armazenamento dos dados diretamente na *Blockchain* (EICHLER *et al.*, 2018), a criptografia dos dados (GEELKERKEN; KONINGS, 2017), a criação de um consórcio *Blockchain*, que garantiria a rastreabilidade de dados confidenciais diretamente

pelos usuários (SATER, 2017, p. 30-31), e o uso de contratos inteligentes que, finalizados, podem ser “mortos”, logo, impedindo-se acesso aos dados gravados na *Blockchain* (NEISSEL; STERI; NAI-FOVINO, 2018). Do mesmo modo, o uso de uma linguagem de descrição para os *logs* de atividades de compartilhamento de dados e ontologias poderá aprimorar os sistemas, assegurando leitura por máquinas e maior transparência (BONATTI *et. al*, 2020).

O quadro a seguir (**Quadro 15**) detalha todos os trabalhos revistados, ano, revista, autores, tema tratado, bem como se os trabalhos apresentam um padrão de descrição de dados, mencionam *Smart Contracts*, preveem em seus sistemas que os *datasets* sejam gravados na *Blockchain*, se descrevem ou não um método para aplicação de suas propostas, as soluções propostas pelos autores e por fim, uma análise, se os trabalhos apresentam um modelo para registro das atividades de compartilhamento de dados.

Quadro 15: Pesquisas revisadas

Código	Nome	Ano	Revista	Autores	Tema tratado	Data análise	Padrão de descrição	Smart contract	Datasets gravados na Blockchain	Descreve um método	Solução	Modelo para registro das atividades de compartilhamento
1	<i>GDPR-Compliant Personal Data Management: A Blockchain-based Solution</i>	2019	<i>IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY</i>	Nguyen Binh Truong, Kai Sun, Gyu Myoung Lee, Yike Guo,	Um modelo para descentralizar consentimentos e logs	25/03/2020	SIM, JSON	Sim	Sim	Sim	Registro descentralizado de autorização de uso de dados e logs, alertando para o risco de estruturas proprietárias no tratamento de dados pessoais	Embora apresente um padrão de descrição, não apresenta um modelo para transferência.
2	<i>Using Blockchain to strengthen the rights granted through the GDPR</i>	2017	<i>INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS"</i>	F.W.J. van Geelkerken, K. Konings	Como a Blockchain pode ser utilizada para armazenar dados garantindo integridade	25/03/2020	Não	Não	Sim	Não	A alternativa para a indeletabilidade seria a criptografia dos dados pessoais com exclusão da chave. Para alterações de dados pessoais inexatos, adição de um bloco com informações atualizadas. Informa que nas blockchains privadas, em se conhecendo os nós, pode-se excluir dados, desde que aprovado pela maioria	Não
3	<i>A Blockchain-based Approach for Data Accountability and Provenance Tracking</i>	2017	<i>ARES '17, Reggio Calabria, Italy</i>	Ricardo Neisse, Gary Steri, and Igor Nai-Fovino	Gestão o consentimetno baseada em contratos	27/03/2020	Não	Sim	Sim	Sim	Propõe a criação de Políticas de Privacidade interativas, com base em contratos inteligentes gravados na Blockchain	Não

4	<i>Blockchain and Data Protection: the value of personal data</i>	2018	Studio Legale Fabiano	Nicola Fabiano	Abordagem sobre os riscos das transações na <i>Blockchain</i>	28/03/2020	Não	Não	Não	Não	Apresenta risco a privacidade em transações na <i>Blockchain</i> . Dificuldade de apagamento e correção de dados	Não
5	<i>Blockchain, data protection, and the GDPR</i>	2018	BlockChain Bunderverband	Natalie Eichler, Silvan Jongerius, Greg McMullen, Oliver Naegele, Liz Steininger, Kai Wagner	A <i>Blockchain</i> e a GDPR, desafios e riscos a privacidade	28/03/2020	Não	Não	Não	Não	Utilização de hashes para pseudonimizar os dados pessoais e criptografia, além de minimização. Classificação dos atores. Soluções para contornar os riscos da violação à privacidade na <i>Blockchain</i>	Não
6	<i>Blockchain and individuals' control over personal data in European data protection law</i>	2017	Não informado	Filippone Roberta	Os desafios do uso da <i>Blockchain</i> em relação as titulares de dados pessoais	28/03/2020	Não	Não	Não	Não	Define a <i>Blockchain</i> na GDPR e informa que soluções descentralizadas seriam melhores para o controle dos titulares. Por outro lado, alerta que <i>Blockchains</i> públicas podem favorecer a centralização, por novas formas de dominância	Não
7	<i>Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem</i>	2018	15th International Joint Conference on e-Business and Telecommunications (ICETE 2018)	Konstantinos Rantos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis and Alexandros Papanikolaou	Apenas mencionaas ontologias, sem descrever	29/03/2020	Não	Sim	Não	Sim	Registro do consentimento na <i>Blockchain</i> por interface mediadora	Não

8	<i>Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows</i>	2016	Não informado	Stan Sater	Aborda os desafios da harmonização entre a <i>Blockchain</i> e a GDPR	29/03/2020	Não	Sim	Sim	Não	Propõe a criação de IDs de usuários que não mais ficam na posse de controladores, mas dos titulares, propondo ainda a criação de um consórcio <i>Blockchain</i> em conformidade como cenário regulatório.	Não
9	<i>The General Data Protection Regulation and Blockchains</i>	2018	University of Helsinki	Cagla Salmensuu	Questões envolvendo proteção de dados e <i>Blockchains</i>	04/04/2020	Não	Não	Sim	Não	Apresenta a tendência para as <i>Blockchains</i> permissionadas e a importância de conhecer as identidades das pessoas que transacionam e dos nodos que validam operações. Posiciona que é mudar o conceito jurídico de apagamento, expandindo o conceito para a desativação de acesso	Não
10	<i>Transparent Personal Data Processing: The Road Ahead</i>	2020	Università' di Napoli Federico I	Piero Bonatti, Sabrina Kirrane, Axel Polleres, Rigo Wenning	Avalia sistemas para registros de <i>log</i> de transações de dados pessoais	08/01/2021	Sim, RDF, PROV5 e OWL-Time6	Não	Sim	Não	Apresenta meios candidatos para registros (<i>logging</i>) das atividades, como elementos centrais envolvendo a privacidade e proteção de dados. Registros locais, registros em terceiros, e registros virtuais <i>p-2-p</i> . Descrevem como vocabulários RDF podem ser usados para representar transferência de dados	Não

Fonte: elaborado pelo autor

Como se pôde constatar, conquanto os trabalhos tragam os desafios e a previsão do uso da *Blockchain*, modelos de contratos eletrônicos, características que um sistema deva ter, até mesmo demonstrando a importância do padrão de descrição de dados para os *logs*, não foram identificadas propostas de modelos para registro das operações de compartilhamento de dados pessoais na *Blockchain*.

Finalizadas as análises da pesquisa envolvendo o uso da *Blockchain* no registro de operações de compartilhamento de dados, passa-se a apresentação do modelo proposto, objeto desta pesquisa.

6 UMA PROPOSTA PARA REGISTRO DESCENTRALIZADO DAS OPERAÇÕES DE COMPARTILHAMENTO DE DADOS PESSOAIS COM BASE NA *BLOCKCHAIN*

Realizada a pesquisa, com base nos aportes identificados, e diante do evidenciado risco à privacidade que os titulares de dados correm com a não transparência nas operações de compartilhamento de dados, considerando ainda que o consentimento nem sempre é considerado a melhor forma de proteção do titular de dados, tendo em vista o crescimento tecnológico e as manobras desleais feitas por controladores para obtê-lo, descreve-se a presente proposta, que se propõe organizar informação sobre transferências de dados, com referências para construção de aplicações de registros transparentes, rastreio e visualização de fluxos de compartilhamentos de dados, de importância social à medida em que aprimorará a privacidade dos titulares de dados, pesquisa esta inserida no contexto da organização e recuperação da informação, processos de estudo e de relevância no Programa de Pós-Graduação em Ciência da Informação (PPGCI).

O modelo conceitual deverá contemplar as seguintes características, consideradas elementos indispensáveis à robustez e precisão:

- a) **Transparência:** permitir ao titular dos dados identificar de forma dinâmica e em um painel quando e para quais agentes os dados foram transferidos. O sistema não deve se basear em dados “já armazenados” onde o titular deve requerer ao controlador que apresente os registros de compartilhamento, pois eles podem ser manipulados e não retratar a realidade;
- b) **Descentralização:** não se pode permitir que os agentes de tratamento digam, de forma unilateral, o que fazem com os dados em suas políticas. Do mesmo modo, não se pode permitir que somente eles armazenem os registros das atividades. Os sistemas de *login*, autenticação ou coleta de dados devem ser descentralizados, impedindo-se manipulações. Como visto na pesquisa, sistemas descentralizados oferecem maior autonomia e privacidade aos indivíduos (FILIPPONE, 2017);
- c) **Rastreabilidade:** o titular dos dados deve ser capaz de visualizar os fluxos de dados remetidos do agente controlador para outros processadores ou outros controladores, e destes para outros, sendo capaz de identificar claramente os fluxos feitos com seus dados, podendo seguir o caminho reverso (identificar a origem do compartilhamento de dados) e garantindo-se que ordens de apagamento se estendam a todos que manipularam os referidos dados, desde que amparadas pela legislação;

- d) **Obrigatório:** as Autoridades de Proteção de Dados precisam definir o padrão como mínimo obrigatório, sendo procedimento em analogia às notas fiscais eletrônicas e documentos Auxiliares da Nota Fiscal Eletrônica (Danfes), onde a transferência de mercadorias sem as mesmas é considerada infração. Se as autoridades continuam com abordagens de “recomendações”, os agentes continuarão com os sistemas atuais, centralizados e não transparentes. Esse é o desafio existente entre o direito e a tecnologia: Operacionalizar tecnicamente o que é previsão legal. Neste aspecto, importante mencionar que a Lei Geral de Proteção de Dados (BRASIL, 2018) confere competência à Autoridade Nacional de Proteção de Dados não só para fiscalizar agentes de tratamento de dados, mas para estimular a adoção de padrões para serviços e produtos que facilitem o exercício do controle dos titulares sobre seus dados pessoais. Tem competência ainda para regulamentar as formas de publicidade das operações de tratamento e editar regulamentos e procedimentos sobre proteção de dados:

Art. 55-J. Compete à ANPD: Incluído pela Lei nº 13.853, de 2019)

IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

III - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; (Incluído pela Lei nº 13.853, de 2019).

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019).

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019). (BRASIL, 2018).

- e) **Auditoria:** o modelo representa um instrumento válido de organização de dados e registro de atividades para proporcionar auditorias e desconformidade. Autoridades poderão facilmente identificar empresas que violam as regras envolvendo compartilhamento de dados pessoais, pois poderão confrontar as políticas (o que é dito nelas) com as operações realizadas na plataforma, que ficam registradas em “logs” das atividades, sem que os controladores tenham o poder de “editar” tais logs;
- f) **Privacidade no design:** apenas o titular dos dados e os agentes de tratamento poderão identificar os registros de transferências, pois, apesar de ficarem gravados

na *Blockchain*, são identificados apenas nestes os códigos das transações e os IDs envolvidos ou chaves públicas, não se identificando tratar de um registro de transferência de dados, o que fica apenas na instância do *Smart Contract* ou da programação que interage com a *Blockchain*. Não deve ser possível, a partir da chave pública do titular, vasculhar a *Blockchain* e identificar por onde seus dados fluem, conseqüentemente, identificar seus hábitos de consumo, *sites* acessados e aplicativos utilizados. O código identificador de rastreamento das atividades de compartilhamento ficará em posse apenas do titular de dados pessoais;

- g) **Linguagem de descrição formal:** os sistemas atuais de registro de consentimentos ou de contratos *online* entre titular de dados e controladores e seus compartilhamentos não possuem uma descrição formal, o que pode prejudicar a recuperação da informação, demandando custos para se processar formatos de diversos controladores, o que colabora para a ausência de transparência e favorece este ambiente de invasão à privacidade. A descrição formal é tratada na pesquisa como um avanço na recuperação da informação sobre compartilhamento de dados por Truong *et al.* (2019) e por Bonatti *et al.* (2020);
- h) **Contornar a problemática da imutabilidade da *Blockchain*:** a proposta a ser construída preservará na *Blockchain* um campo contendo os *hashs* dos *datasets* (*conjunto de dados*) remetidos, e o controlador preservar igualmente o *hash* do *dataset* em sua posse. Assim, diante de uma auditoria, bastaria ao titular ou Autoridade de Proteção de Dados exigir detalhes sobre um *hash* de banco de dados específico, transacionado e público em um dia e hora no painel visualizador a partir do endereço público do controlador e do processador ou terceiro. Este, então, colaboraria apresentando os dados (cujo *hash* deve ser o mesmo), indicando igualmente os dados dos titulares envolvidos. O titular consultaria as atividades com seus dados (ou *datasets* que contém seus dados) não a partir de sua chave pública na *Blockchain*, mas com base em um ID único de rastreamento previsto em seu *Smart Contract*, de conhecimento privado. **Ou seja, se o titular cria um *Smart Contract*, receberá um ID único diverso da sua chave pública, e este ID é associado a versões de contratos transacionados com as bases dos controladores com quem se relaciona, permitindo-se assim que este consiga rastrear seus dados executando seu contrato, ao mesmo tempo, não revelando na *Blockchain* seu endereço público tampouco seus dados pessoais, o que poderia implicar em violações de privacidade.**

Assim, não haveria problema de registros de transação permanecerem na rede (já que em tese os registros são indelévels em *Blockchains*) pois não revelam a identidade do titular, não revelam os dados do titular, mas o *hash* do *dataset* enviado, apresentando apenas os endereços públicos dos controladores e processadores, sendo possível identificação rápida de fluxos de dados, sem associação direta a pessoas.

Os atores no sistema proposto são:

- a) **Titular de dados (TD):** é o dono dos dados, e que fornece os referidos dados de modo consciente ou inconsciente ao responsável pelo tratamento de dados;
- b) **Agente controlador (AC):** é o agente de tratamento de dados pessoais, linha de frente com o titular de dados, tendo coletado dados pessoais de forma espontânea pelo titular ou mesmo dados que o titular desconhece que são coletados. Ele pretende fazer o compartilhamento de dados, com ou sem o consentimento do titular, de acordo com sua análise das premissas legais;
- c) **Agente processador/outros controladores (AP):** são agentes de tratamento terceiros, que recebem os dados compartilhados do Agente controlador para tratamento segundo finalidades informadas ou outros controladores que tratam dados pessoais;
- d) **Agentes diversos (AD):** são demais agentes de tratamento, como autoridades, auditores.

A organização da informação e o modelo proposto deverá se organizar da seguinte forma:

- a) Ao utilizar uma plataforma de um agente de tratamento de dados, o titular de dados enviará seu *Smart Contract*, contrato inteligente que será executado diante de compartilhamentos;
- b) Dados sobre o compartilhamento de dados são gerados a partir do *trigger* ou gatilho de compartilhamento, presente nas aplicações que utilizarem o modelo. A partir do *dataset* selecionado, metadados sobre o *datasets* são descritos e integram os dados sobre o compartilhamento, em linguagem estruturada; Estes metadados incluem data, hora, quem receberá os dados e formato;

- c) A partir da geração do registro, ocorre a autenticação no contrato eletrônico, com capacidade de gravar os dados no “*ledger*”, que registrará apenas os dados em formato pseudonimizado, registro da transação envolvendo o compartilhamento. Caso o consentimento seja necessário, antes da gravação, o titular será notificado para acessar o contrato e verificar uma solicitação de compartilhamento de dados. Caso contrário, a operação será feita e o registro gerado. Esses registros servirão de prova, inclusive, para se questionar compartilhamentos cujo titular entenda que deveria ter consentido;
- d) A partir desta chamada e gravação na *Blockchain*, o titular conseguirá, a partir do seu ID único de rastreio, acessar informações sobre transferência de seus dados, a agentes de tratamento com os quais o controlador tenha compartilhado o mesmo. Na *Blockchain*, não serão armazenados os *datasets* e categorias de dados, mas um *hash* que conectado com a base do controlador, pode comprovar quais dados foram compartilhados.

Identificados os requisitos que o modelo deverá conter, características, atores e como a organização da informação se dará no modelo, apresentam-se a sistemática do modelo e os passos de seu funcionamento, incluindo os fluxos existentes entre os atores envolvidos no compartilhamento de dados pessoais, de modo a permitir a fácil operacionalização do modelo, por meio de soluções computacionais que considerem a tecnologia *Blockchain*.

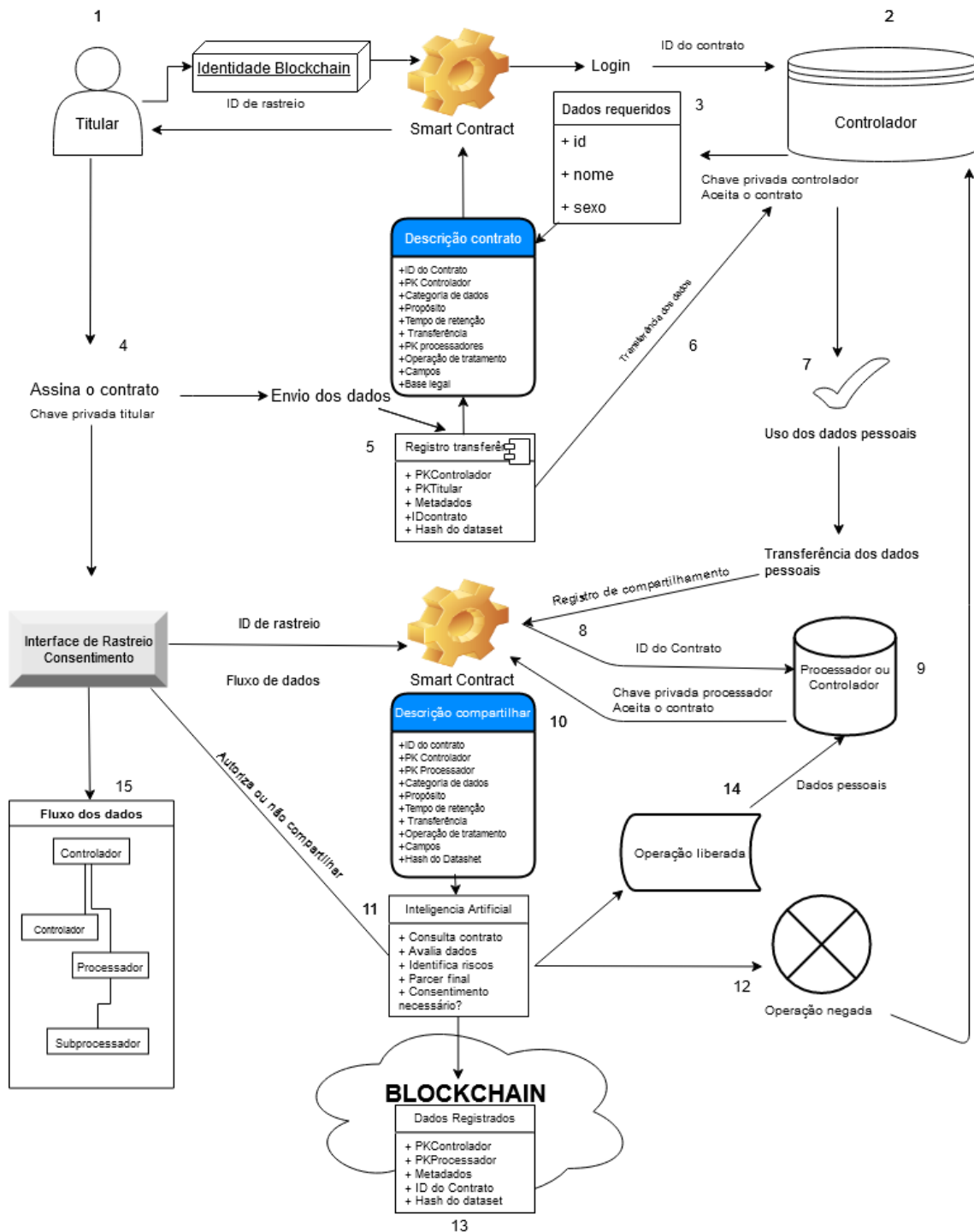
- a) O (AT) Agente de tratamento adere ao *Smart Contract* do titular, a partir deste momento recebendo um endereço imutável que o identifica no contrato de compartilhamento de dados do titular;
- b) O (TD) titular dos dados também adere ao *smart contract* a partir do seu ID, sendo assim receberá um contrato único. Este ID sequer o agente de tratamento terá;
- c) Os AT podem permitir que os TD realizem *login* ou cadastro em suas aplicações a partir de um endereço no sistema descentralizado, não mais custodiando dados pessoais do TD;
- d) Estabelecendo-se uma transação que exija o tratamento de dados pessoais é gerado um registro de primeira transferência. O registro terá um código da transação e seus metadados são **(ID do contrato, Chave pública do controlador, categoria de dados, propósito ou finalidade do tratamento, tempo de**

- retenção, transferência, chaves públicas dos processadores, operação de tratamento, campos, base legal).** Outros campos podem ser adicionados;
- e) Quando o AT Controlador for realizar uma transferência para o AT Processador ou para o AD Diversos, uma transação será gerada na modalidade compartilhamento de dados; o registro terá um código de transação e seus metadados são **(ID do contrato, chave pública do controlador, chave pública do processador/terceiro destinatário, categoria dos dados, propósito, tempo de retenção, transferência, operação de tratamento, campos, hash do dataset).** Outros campos podem ser adicionados;
 - f) Neste sentido o titular de dados TD (Titular de dados) será instantaneamente notificado para “consentimento dinâmico” para aprovar ou não a transferência (caso o código base de dados seja “consentimento”), poderá rapidamente navegar (*links*) pelos códigos de transações, identificando os agentes que receberam seus dados, data, qual o conteúdo do *dataset*, se existiam dados sensíveis dentre outros, em “painéis dinâmicos” criados a partir da organização dos dados e uso do modelo. O *Smart Contract* tem a capacidade de resolver a pseudonimização identificando quem é a empresa responsável por um ID que recebeu os dados. Logo, quem acessar a rede pública verá que houve transações de um *hash*, a partir de um ID, para outro ID. Somente através do contrato e com o ID do Titular será permitido verificar/reassociar os IDs aos dados, identificando os atores envolvidos;
 - g) Uma ordem de exclusão de dados também deverá gerar um registro e a comprovação poderá ser registrada como uma transação;
 - h) Agentes diversos (AD) poderão auditar com facilidade os fluxos de dados, e efetivamente conhecer quais os compartilhamentos existentes, considerando que o sistema descentralizado impede que os ATs façam ocultações ou omitam as operações de compartilhamento, pois será possível identificar comportamentos anômalos para as atividades informadas pelos Controladores, como por exemplo, um controlador que “nunca registrou uma atividade de compartilhamento de dados”, poderá gerar um alerta de uma ocultação ou contorno do modelo.

Demonstra-se relevante, como pesquisa futura, ampliar os estudos de metadados, a fim de se criar ontologias que possam enriquecer todos os dados do processo, e permitam melhor estruturação e futura recuperação da informação.

Apresenta-se o gráfico e fluxos do modelo proposto (**Figura 28**):

Figura 28: Modelo Conceitual para Rastreo de Atividades de Compartilhamento de Dados Pessoais



Fonte: elaborado pelo autor

Pela sistemática do modelo proposto:

- 1) O Titular de dados pessoais terá uma identidade na *Blockchain*, vinculada a *Smart Contracts* de diversos controladores; terá também um ID de rastreo, número que não será negociado com ninguém além do próprio titular e que permite visualizar o compartilhamento de dados em cada contrato com controladores;
- 2) Quando o titular pretender usar um serviço enviará o *Smart Contract* ao Controlador de dados que o assinará;
- 3) O Controlador então informará no *Smart Contract* os dados necessários, assinando o mesmo com a chave privada;
- 4) O titular também assina o contrato;
- 5) Ocorre o registro do contrato na *Blockchain* (PK (chave pública) Controlador, PK Titular (chave pública), Metadados como data, hora, IDcontrato, *Hash* do *dataset*);
- 6) Os dados são transferidos ao controlador;
- 7) O controlador utiliza os dados pessoais.

Diante de uma atividade de compartilhamento de dados para processadores ou outros controladores, tem-se:

- 8) Um novo registro é solicitado ao contrato;
- 9) O ID do contrato é enviado ao controlador ou processador que receberá os dados; O controlador ou processador assina e aceita o contrato;
- 10) A descrição do contrato é formada com os campos necessários relativos ao compartilhamento;
- 11) Neste momento, agentes computacionais e assistentes de privacidade (*Personal Privacy Assistants*) poderão atuar sobre o contrato avaliando riscos, liberando ou não o compartilhamento. Quando o consentimento for necessário o titular será alertado em sua interface de rastreo/consentimento;
- 12) Caso a operação seja negada, o controlador será informado;
- 13) Se autorizada, ou não necessitar de consentimento, a transação será registrada na *blockchain* (PKControlador, PKProcessador, Metadados (Data, hora, finalidade), ID do Contrato, *Hash* dos *datasets*);

- 14) Os dados são transmitidos ao Processador/Controlador destinatário;
- 15) Na Interface de Rastreamento/Consentimento o Titular de Dados poderá acompanhar os fluxos com seus dados pessoais.

Neste sentido, endereça-se, com o modelo conceitual proposto, uma deficiência identificada nas pesquisas, envolvendo a ausência, na legislação ou nos códigos de boas práticas, de modelos que organizem as informações sobre compartilhamento de dados, na construção de soluções que efetivamente devolvam ao titular o controle sobre seus dados pessoais, aumentando a sua privacidade e facilitando auditorias por entidades reguladoras, empresas e órgãos públicos e de fiscalização.

7 CONSIDERAÇÕES FINAIS

Considerando a constatação das dificuldades de titulares de dados pessoais em conhecerem quem tem acesso a seus dados pessoais, esta pesquisa investigou quais os direitos trazidos pelos regulamentos Brasileiro e Europeu sobre compartilhamento de dados pessoais, averiguando igualmente as melhores práticas já lançadas sobre compartilhamento de dados, suas disposições e omissões. Avaliou-se ainda a transparência de 5 (cinco) redes/aplicativos populares no Brasil e mundo, identificando como efetivamente tratam as questões envolvendo compartilhamento de dados pessoais e o nível de transparência que oferecem ao titular dos dados acerca destas atividades.

Além disso, estudou-se como mecanismos descentralizados, como a *Blockchain*, a princípio usada para suportar transações em criptomoedas, vem sendo utilizada para guarda de registros, considerando os riscos à privacidade e como o registro dos compartilhamentos de dados pode se valer desta tecnologia contornando seus desafios.

De modo a orientar a pesquisa, foi identificado o **objetivo geral** e **sete objetivos específicos**. O objetivo geral consistiu na proposta de criação de um modelo conceitual para descrição, registro e recuperação das operações de compartilhamento de dados na *Blockchain*, a partir da caracterização da grave violação a privacidade decorrente da assimetria informacional e obscuridade sobre as reais operações de compartilhamento de dados realizadas por agentes de tratamento de dados pessoais.

Foram **objetivos específicos** do presente trabalho, identificar o conceito de “compartilhamento de dados” no Ciclo de Vida dos Dados; avaliar quais os direitos trazidos aos titulares de dados pessoais na Lei Geral de Proteção de Dados e *General Data Protection Regulation*; identificar guias, procedimentos e códigos de prática envolvendo compartilhamento de dados pessoais; avaliar como o compartilhamento de dados pessoais vem sendo descritos nas Políticas de Privacidade e se contemplam a transparência mínima sobre descrição dos fluxos de dados, bem como se as aplicações estão atendendo requerimentos a respeito de informações sobre quais entidades compartilham dados; identificar quais os riscos a privacidade e para o exercício dos seus direitos decorrentes da opacidade do titular em conhecer as operações de compartilhamento dos seus dados; caracterizar o ambiente da pesquisa envolvendo *Blockchain* e o registro de transações; apurar como os compartilhamentos de dados poderão ser rastreados pelo titular dos dados com a organização e registro de dados na *Blockchain*; propor um modelo de organização e recuperação das informações relativas

ao compartilhamento de dados pessoais, proporcionando transparência ao titular de dados no acesso às operações de compartilhamento de seus dados.

O **Capítulo 2** enfrentou as respostas para atendimento aos objetivos específicos 1 e 2 (“Identificar o conceito de “compartilhamento de dados” no Ciclo de Vida dos Dados” e “Avaliar quais os direitos trazidos aos titulares de dados pessoais na Lei Geral de Proteção de Dados e *General Data Protection Regulation*”) onde investigou-se a conceituação de dados pessoais, bem como o conceito de compartilhamento de dados nos regulamentos e no Ciclo de Vida dos Dados, de Sant’Ana (2016), compreendendo suas diversas denominações.

Com constatado (**Quadro 4**, p. 44) não existe uma uniformização das denominações que designam nos regulamentos estudados e no Ciclo de Vida dos Dados, a atividade envolvendo “compartilhamento”, o que pode gerar interpretações diversas e subjetivismos.

Este objetivo demonstrou-se válido, pois, a adoção de um padrão para registro de atividades de compartilhamento passa pela compreensão do que consiste na atividade de tratamento denominada “compartilhar”. Também se demonstrou o desafio envolvendo a atividade anonimização de dados, que não pode ser realizada de qualquer modo, mas deve assegurar a irreversibilidade de associação do dado a seu titular.

Detalhou-se quem são os atores ou figuras previstas na legislação envolvendo proteção de dados pessoais (**Quadro 5**, p. 50), também estabelecendo um comparativo entre as Legislações Brasileira, Europeia e CVD. Foram investigados os princípios de proteção de dados pessoais, as fases geracionais de legislações envolvendo proteção de dados, e buscou-se avaliar quais os direitos trazidos aos titulares de dados pessoais, na Lei Geral de Proteção de Dados, quanto na *General Data Protection Regulation* (GDPR). Como constatado, os princípios que tutelam os titulares de dados para conhecerem dados e informações sobre compartilhamento de seus dados pessoais foram identificados na legislação Brasileira como: livre acesso, transparência e responsabilização e prestação de contas. Já na legislação Europeia, tal direito encontra guarida nos princípios da licitude, lealdade e transparência. Do mesmo modo, identificou-se no **Capítulo 2** as premissas para tratamento de dados pessoais, ou seja, as condições pelas quais um agente de tratamento está habilitado a realizar o tratamento, incluindo o compartilhamento.

Foi identificado que embora não haja a necessidade do consentimento em algumas hipóteses previstas na legislação, fato é que se outras operações forem realizadas ou os dados forem compartilhados para terceiros, o consentimento poderá ser necessário para

estas operações específicas. Em outras hipóteses, ainda, envolvendo consentimento dispensável para compartilhamento, o titular permanece no direito de ter informações sobre “com quem” o controlador compartilhou seus dados.

Investigou-se como é tratado o “compartilhamento de dados” nas legislações e se os regulamentos LGPD e GDPR contemplam o direito de conhecer os agentes com quem o controlador compartilhou dados. Na GPDR, tais direitos foram identificados nos artigos 15 e 30. Já na LGPD, no art. 9, que estabelece que o titular tem direito de acesso facilitado a informações acerca do uso compartilhado de dados pelo controlador e a finalidade. No entanto, a Lei não especifica, como este acesso se dará, o que pode tornar este direito não instrumentalizado.

O objetivo específico 3 (Identificar guias, procedimentos e códigos de prática envolvendo compartilhamento de dados pessoais) foi atendido no **Capítulo 3**, onde ao investigar os procedimentos, códigos de prática e guias envolvendo compartilhamento de dados pessoais, de autoridades e entidades de diversos países, observou-se que todos estão preocupados com a transparência dos compartilhamentos de dados sem, contudo, estabelecerem protocolos ou padrões para que estes dados ou fluxos de compartilhamentos possam ser facilmente identificados pelo titular dos dados. Agrupou-se então o conteúdo dos códigos em itens: a) transparência; b) acompanhamento do ciclo de vida e fluxos de compartilhamento; c) contratos de tratamento de dados; d) novos agentes de tratamento devem gerar comunicações ao titular; e) painéis de proteção de dados; f) consentimentos dinâmicos; g) uso da *blockchain*; e h) dados necessários para solicitação de compartilhamento de dados. De todos os códigos revisados, O *Trusted Data Sharing Framework (2019)* é o único Código que trata da *Blockchain* ou dos registros não centralizados para aumentar a transparência ao titular dos dados pessoais nas operações de compartilhamento. As soluções “descentralizadas”, como a tecnologia de contabilidade distribuída, estão possibilitando novos modelos de troca de dados, mercados e serviços como verificação de dados, segurança e certificação, contratação e governança.

Por sua vez, o Código de Boas Práticas publicado em 17 de dezembro de 2020, *Data Sharing code of practice* (ICO, 2020a), prevê um Anexo B, onde estabelece um padrão de solicitação de compartilhamento de dados, a ser usado por organizações, contendo dados necessários para ciência ao titular em casos em que haja a necessidade de consentimento. Também apresenta elementos para que controladores de dados avaliem

se devem ou não compartilhar dados pessoais, o que considera dados e informações a serem cadastradas no formulário disponibilizado.

No **Capítulo 4** foi atendido o objetivo específico 4 “(Avaliar como o compartilhamento de dados pessoais vem sendo descritos nas Políticas de Privacidade e se contemplam a transparência mínima sobre descrição dos fluxos de dados, bem como se aplicações estão atendendo requerimentos a respeito de informações sobre quais entidades compartilham dados)”; onde se investigou como as aplicações *Google*, *Strava*, *Samsung*, *Facebook* e *WhatsApp* tratavam requerimentos envolvendo informações sobre compartilhamentos de dados.

Avaliou-se, assim, aplicações de uso no Brasil, especificamente, no que diz respeito à transparência oferecida ao titular de dados pessoais sobre as atividades de compartilhamento que são feitas com seus dados. Como verificado, nenhuma das empresas indiciou de forma precisa as empresas e controladores que receberam os referidos dados, bem como quais, como e quando os dados foram compartilhados. Constatou-se também que nenhuma das redes analisadas ofereceu a possibilidade, mesmo requeridas, de se ter acesso ao nome e identidade dos agentes com quem compartilham os dados (**Quadro 11**, p. 112).

Ainda no **Capítulo 4**, tal constatação evidenciou o objetivo 5 da pesquisa (Identificar quais os riscos à privacidade e para o exercício dos seus direitos decorrentes da opacidade do titular em conhecer as operações de compartilhamento dos seus dados), que foi identificar os riscos atuais para a privacidade e para o efetivo exercício dos direitos dos titulares de dados pessoais, previstos na legislação. Como observou-se, existe uma distância entre a previsão legal de princípios que protegem o titular de dados pessoais diante de compartilhamentos não autorizados e o efetivo exercício dos direitos, com uma lacuna de metodologias e procedimentos, operacionalizados pela computação, que facilitem a este conhecer controladores que acessam seus dados.

Os sistemas atuais de proteção e mera previsão dos direitos dos titulares não são capazes de prover aos mesmos a transparência necessária para que conheçam as requisições de compartilhamento, as autorizem ou não, ou mesmo identifiquem os fluxos dos dados pessoais, que são feitos pelos agentes de tratamento que obtém acesso aos referidos dados.

Como visto, a Legislação *General Data Protection Regulation*, e a Lei Brasileira, definem princípios e garantias ao titular dos dados. Ambas as legislações asseguram acesso aos dados e total transparência nas operações de tratamento, o que envolve, o

compartilhamento. No entanto, as Leis carecem de regulamentação e instrumentalização destes direitos, o que pode ser sanado com o modelo proposto nesta pesquisa. Como constatou-se, não se tem uma única forma de se “demonstrar transparência”, o que favorece o cenário de desrespeito nas aplicações pesquisadas, muitas que sequer respondem às solicitações de informações. Dificuldades de solicitar informações sobre compartilhamento de dados foram identificadas na totalidade das aplicações. Em três, não fora possível sequer realizar contato. Percebe-se até o momento que somente com as Legislações, recentemente sancionadas, não se obterá uma melhora sensível na transparência aos titulares de dados.

Os Códigos de boas práticas revisados indicam tentativas de uniformizar e aprimorar a transparência das operações de compartilhamentos, no entanto, com enfoque jurídico e negligenciando o técnico/informacional, são superficiais em questões operacionais a respeito de compartilhamentos de dados pessoais, como por exemplo, a organização, descrição dos dados que serão compartilhados e como o titular poderá recuperar estes fluxos. O Código Inglês, de dezembro de 2020 (ICO, 2020a) avança, e começa a descrever dados necessários para requerimento de compartilhamento de dados e dados necessários para avaliação da decisão sobre compartilhar ou não. Porém destina-se apenas aos casos em que o compartilhamento dependa do consentimento do titular de dados, embora tenha contribuído com dados importantes e que podem servir de referência para registros de atividades de compartilhamento e automatização de decisões relativas a compartilhamentos, a partir de parâmetros pré-definidos por agentes de tratamento e titulares.

Evidenciou-se que embora o consentimento venha previsto como uma das premissas para tratamento de dados pessoais, não se tem, claramente, procedimentos, métodos que descrevam o meio, o formato e em quais fases do tratamento de dados tal consentimento deva ser solicitado. Observou-se igualmente que nem sempre o consentimento será necessário para o compartilhamento de dados, o que não retira dos agentes de tratamento o dever de prestar informações claras aos titulares sobre terceiros que recebem seus dados pessoais e quais dados são estes. Controladores esforçam-se em suas políticas de privacidade para preverem o compartilhamento de dados, mas não são claros acerca dos dados compartilhados, frequência, e a identidade dos que recebem os dados pessoais. Ainda que controladores declarem que não realizam compartilhamentos, não se poderá ter a certeza de que não o fazem, pois os controladores centralizam o

compartilhamento de dados, não existindo um padrão descentralizado, que permita transparência e auditoria.

Com base nas pesquisas realizadas, identificou-se que uma estrutura cliente-servidor de gestão e compartilhamento de dados pessoais, comum em todas as aplicações pesquisadas, que são aplicações com grande densidade de titulares de dados em todo o mundo, jamais poderá oferecer a transparência necessária para auditorias das Autoridades de Proteção de Dados.

Neste contexto, também foi o sexto objetivo específico da pesquisa identificar pesquisas envolvendo a tecnologia *Blockchain* no registro de transações, nomeadamente, caracterizar a pesquisa envolvendo registro de operações de compartilhamento de dados. O **Capítulo 5** endereçou este tema (caracterizar o ambiente da pesquisa envolvendo *Blockchain* e o registro de transações), onde inicialmente conceitua e traz um panorama do desenvolvimento da tecnologia *Blockchain* e suas características. Posteriormente ingressa-se nos desafios, a partir de diversas óticas para a tecnologia e na classificação da *Blockchain*. Observou-se, da revisão de trabalhos sobre o tema, que a pesquisa ainda é incipiente, porém os mecanismos descentralizados e distribuídos restam evidenciados como mecanismos que retiram do controlador a “ditadura dos dados”, aumentando a transparência para titulares e dificultando fraudes, manipulações e tratamentos indevidos. Do mesmo modo, tratou-se da revisão dos impactos de tecnologias descentralizadas, como a *Blockchain*, na privacidade dos indivíduos, bem como desafios para harmonização das plataformas com direitos relativos à privacidade, como exemplo, o direito a exclusão de dados.

Identificou-se ainda que: a) tanto a legislação Brasileira como Europeia contemplam princípios que asseguram ao titular o direito de conhecer as pessoas com quem se compartilham dados; b) a preferência da legislação Europeia por um “sistema eletrônico” que possibilite ao titular aceder diretamente a seus dados pessoais; c) a ausência, nos códigos e melhores práticas, de uma metodologia para registro das atividades de compartilhamento; d) ausência de transparência nas aplicações pesquisadas, mesmo após requeridas informações sobre compartilhamentos de dados; e e) o potencial da tecnologia *Blockchain* para modificar o atual cenário oferecido pelos agentes de tratamento, em estruturas centralizadas, onde fica dificultoso identificar o que realmente é feito com os dados pessoais.

Mesmo com características aparentemente conflitantes, como a “indeletabilidade” dos dados, foi possível identificar que este não deve ser visto como um problema para

adoção da tecnologia, com propostas científicas como limitação do acesso aos dados gravados, a adição de *Blockchains* permissionadas, geração de *hashing* dos *datasets* e não armazenamento, criptografia dos dados, ou mesmo a criação de um consórcio *Blockchain*, que permitiria aos usuários o rastreamento de seus dados. Mais que isso, a *Blockchain* favorecerá não apenas a organização e o registro de operações de compartilhamento, para com a organização de dados e metadados sobre as atividades, o que facilitará auditorias, mas para a possibilidade da geração de políticas de privacidade interativas, com base em contratos inteligentes e de leitura por dispositivos computacionais, **podendo-se estabelecer futuros assistentes pessoais de privacidade, códigos com capacidade de tomada de decisão pelo titular, suprimindo seu desconhecimento em compreender o que é feito com seus dados pessoais.** Estes contratos poderão ser pré-programados por controladores e titulares e se auto executarão satisfecitas determinadas condições. Um contrato poderá, de acordo com os critérios, negar o compartilhamento de dados pessoais, ou informar o titular em seu *e-mail*, sempre que uma operação de compartilhamento se realizar, com avisos, recomendações e advertências.

Com base nos estudos realizados no **Capítulo 5**, chegou-se à conclusão que as aplicações que surjam com a finalidade de registrar, de forma descentralizada ou como agentes intermediários, as operações de tratamento, deverão: a) remover do controlador a posse destes registros; b) ser baseado em linguagem de descrição padronizada e organizada; e c) utilizar técnicas para evitar violações a direitos dos titulares de dados pessoais, como por exemplo, considerar alternativas para assegurar que o direito a exclusão dos registros (ou o não acesso a eles) possa ser exercido.

Considerando o aporte teórico identificado e revisado na pesquisa, foi objetivo específico 7 da pesquisa, a propositura de um modelo de organização e recuperação de informações relativas a compartilhamento de dados pessoais, com base na *Blockchain*, o que foi tratado no **Capítulo 6**.

O modelo proposto, vale-se da característica da *Blockchain* que é distribuída, removendo dos controladores a possibilidade de “ocultarem” ou não informarem compartilhamentos realizados. A proposta poderá ser executada não só por agentes públicos, fiscais e entidades reguladoras, para servir como um padrão para controladores que pretendam compartilhar ou fazer uso de dados compartilhados. Explicou-se assim as características que o sistema deverá ter, os atores que fazem parte do sistema proposto (Titular de dados (TD) e Agente controlador (AC), Agente processador/terceiro (AP), Agentes diversos (AD)).

Do mesmo modo, registrou-se que para a eficácia do sistema ele precisa ser descentralizado e também de uso obrigatório, sendo análogo às notas fiscais eletrônicas, onde a transferência de mercadorias sem as mesmas é considerada infração.

Descreveu-se, igualmente, como se dará a organização da informação no sistema, onde os dados sobre o compartilhamento de dados são gerados a partir do gatilho compartilhamento, e extraídos metadados dos *datasets*, que são gravados de forma pseudonimizada na *Blockchain*. Com a gravação no contrato eletrônico o titular poderá, a partir do seu ID único, acessar as informações sobre transferências de seus dados. No **Capítulo 6** é também apresentado o Modelo Conceitual para Rastreo de Atividades de Compartilhamento de Dados Pessoais, que contará com “Interface de Rastreo” para que titulares acompanhem as operações, bem como para que Agentes diversos (AD) possam auditar os fluxos de dados, fiscalizando se os controladores estão realmente cumprindo ou não a legislação.

Sendo o escopo do trabalho definido, os objetivos da pesquisa foram plenamente atendidos, com a comprovação de que uma proposta para rastreo das atividades de compartilhamento de dados, com base na *Blockchain*, mecanismo descentralizado de registro de atividades, contribuirá com a solução dos problemas identificados nos **Capítulos 2 e 3**.

A tese proposta revela importante contribuição para o desenvolvimento científico, tecnológico, cultural, social e de inovação, como se expõe:

- a) Científico:** apresenta-se como a organização da informação sobre compartilhamento de dados suprimindo uma grave lacuna que impede que titulares de dados pessoais identifiquem os seus fluxos, servindo de base para a construção de soluções que proponham organizar e recuperar tais informações, hoje não acessíveis com facilidade;
- b) Tecnológico:** a concepção de tecnologias para contornar a problemática da opacidade nas operações de compartilhamento de dados se torna eficiente com a estruturação de um modelo conceitual, evitando-se soluções diversas e não padronizadas. Além disso, avalia-se a *Blockchain* como uma tecnologia com potencial para transparência nas operações com dados pessoais, graças a sua característica descentralizada;
- c) Cultural:** o modelo conceitual proposto apresenta-se como elemento fortalecedor da cultura da privacidade e proteção de dados, pois operacionalizado, evidencia à titulares de dados o quão difícil é exercer na prática seu direito de conhecer por onde seus dados andam. Com o modelo, titulares passam a ter ferramentas para acompanhar compartilhamento de dados, o que os aproximará dos direitos previstos em lei, bem como

potencializará a conscientização sobre a necessidade de proteger, monitorar e controlar dados pessoais;

d) Social: a contribuição social da tese é evidenciada pelo elo que une direitos previstos em lei à sua concretização prática, permitindo que a proteção de dados, como direito fundamental, seja exercida em sua plenitude, especialmente, garantindo-se que não haja condutas desleais e omissões de agentes de tratamento sobre os reais destinatários dos dados pessoais, assegurando que os direitos previstos na Lei Geral de Proteção de Dados não sejam apenas expressão legislativas, sem meios para serem exercidas;

e) Inovação: a contribuição da tese com a área da inovação é demonstrada à medida em que se apresenta uma solução para a problemática da visualização dos fluxos de dados, o que possibilitaria a criação de outros modelos e propostas que atuem na recuperação de informações e forneçam elementos práticos para cidadãos exercerem seus direitos, como por exemplo, o modelo pode ser adaptado para usar a *Blockchain* para registrar não só os compartilhamentos, mas todos os consentimentos que um titular de dados forneceu *online*, ou para futuras “Políticas de privacidade interativas”, onde são extraídos, de textos de políticas, quais direitos são assegurados e quais não, permitindo aos titulares rápida visualização e compreensão dos termos. Assim, a proposta descrita na tese fornece elementos para que outras propostas inovem no sentido de organizar informações relativas à privacidade e dados pessoais, ampliando o controle dos cidadãos sobre seus dados pessoais.

Dentre os benefícios identificados com o modelo proposto na pesquisa, estão:

- 1) A padronização de informações sobre atividades de compartilhamento de dados;
- 2) A criação de um mecanismo descentralizado para “registro das atividades”, possibilitando ao titular maior controle sobre atividades de dependam do seu consentimento ou informação precisa nas atividades que não dependam;
- 3) O modelo proposto permitirá que autoridades de proteção de dados, governos e outros controladores realizem auditorias sobre o cumprimento da legislação, que deixam de se embasar apenas em “declarações” de controladores de dados, mas, no que diz respeito a compartilhamento de dados pessoais, serão constatáveis;
- 4) O sistema dará ciência ao titular de dados das transferências internacionais, oferecendo-lhe, ressalvadas as disposições legais, meios para barrar referidos compartilhamentos.

A melhora sensível da transparência das operações de tratamento de dados pessoais está diretamente ligada a utilização pelos agentes de tratamento de dados pessoais de um modelo de descrição descentralizado, como o modelo proposto, com linguagem estruturada para atuação de agentes computacionais, razão pela qual se demonstra relevante que Autoridades de Proteção de Dados estabeleçam padrões obrigatórios ou mesmo que a legislação se atualize, no sentido da compreensão de que soluções atuais, onde somente os Agentes de tratamento detém o controle e a visualização dos dados e registros de compartilhamento, não são capazes de permitir a transparência necessária para que o titular, efetivamente, se beneficie dos direitos previstos nas leis de proteção de dados.

Neste contexto, esta pesquisa objetivou contribuir com a solução desta problemática, ao demonstrar que somente a legislação não é suficiente para que os direitos estampados sejam cumpridos, ao apresentar a ausência de informações claras por parte de aplicações sobre atividades de compartilhamento, após receberem os dados, bem como ao propor um modelo para descrição registro descentralizado de operações de tratamento, com base na *Blockchain*, proporcionando a titulares de dados total conhecimento dos fluxos de seus dados pessoais, sem a necessidade de requererem informações aos agentes de tratamento, modelo que evidencia nítido benefício social, à medida em coíbe a corrupção e transferência indevida de dados pessoais e fornece importantes registros para permitir que agentes regulatórios e de fiscalização possam auditar o efetivo cumprimento da Lei, reduzindo-se a distância entre os direitos previstos e a garantia prática aos mesmos.

7.1 SUGESTÕES PARA TRABALHOS FUTUROS

São sugeridas as seguintes propostas de pesquisa para estudos futuros:

1 – Identificar a matriz de responsabilidades entre controladores e operadores de dados pessoais nas atividades de compartilhamento, com base na revisão de contratos de processamento;

2 – A partir dos requerimentos de informações sobre compartilhamento de dados, desenvolver um observatório de avanços de iniciativas para maior transparência envolvendo atividades de compartilhamento;

3 – Operacionalizar o modelo proposto por meio da programação de um *Smart Contract* (contrato inteligente) autoexecutável, que considerando parâmetros pré-estabelecidos entre titulares de dados e controladores, bem como as exigências legais, atue na tomada de decisões envolvendo o compartilhamento de dados pessoais, inclusive, realizando os registros das atividades;

4 – Considerando as categorias de dados pessoais, como os dados pessoais sensíveis, estabelecer no modelo proposto condicionantes que avaliam a natureza dos dados e sinalizam dispositivos legais e alertas, a partir da criticidade dos mesmos, enviados ao titular;

5 – Com base na mesma estrutura descentralizada proporcionada pela *Blockchain*, desenvolver políticas de privacidade dinâmicas, onde se pode não apenas ter informações sobre como os agentes de tratamento tratam os dados, mas já acessar informações que digam respeito ao titular de dados pessoais, incluindo atividades de compartilhamento de dados pessoais;

6 – Avançar na estruturação dos sistemas que farão a leitura dos dados dos *Smart Contracts* e, com base em inteligência artificial, possam funcionar como assistentes pessoais de privacidade, avaliando riscos, alertando titulares e até tomando decisões para este, em termos de proteção de dados pessoais, suprimindo a dificuldade de titulares em entenderem os riscos do tratamento de dados.

REFERÊNCIAS

ACCENTURE. **The ethics of data sharing**: a guide to best practices and governance. Mountain View: Accenture Technology, 2016. Disponível em: https://www.accenture.com/_acnmedia/pdf-35/accenture-the-ethics-of-data-sharing.pdf. Acesso em: 12 jul. 2020.

AFFONSO, E. P. **A insciência do usuário na rede na fase de coleta de dados: privacidade em foco**. 2018. Orientador: Ricardo César Gonçalves Sant’Ana. Tese (Doutorado em Ciência da Informação) – Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, 2018. Disponível em: https://www.marilia.unesp.br/Home/Pos-Graduacao/CienciadaInformacao/Dissertacoes/affonso_ep_do_mar.pdf. Acesso em: 02 jun. 2020.

AGÊNCIA BRASIL. Saiba quais foram os aplicativos mais baixados no Brasil e no mundo. **Exame**, São Paulo, 19 jan. 2020. Disponível em: <https://exame.abril.com.br/tecnologia/saiba-quais-foram-os-aplicativos-mais-baixados-no-brasil-e-no-mundo/>. Acesso em: 02 mai. 2020.

AKERLOF, G. A. The market for “lemons”: quality uncertainly and the market mechanism. **The Quarterly Journal of Economics**, Cambridge, v. 84, n. 3, p. 488-500, Aug. 1970. Disponível em: <http://socsci2.ucsd.edu/~aronatas/project/academic/Akerlof%20on%20Lemons.pdf>. Acesso em: 10 jul. 2020.

ANPD Autoridade Nacional De Proteção De Dados. **Institucional**: estrutura organizacional. 2020. Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional>. Acesso em: 8 jan. 2021.

AUDY, J. K. **William Edwards Deming (1900-1993)**. Jorge Horácio “Kotick” Audy, jan. 2016. Disponível em: <https://jorgeaudy.com/2016/01/27/william-edwards-deming-1900-1993/>. Acesso em: 02 jun. 2020.

BARKER, C. 25 billion connected devices by 2020 to build the Internet of Things. ZDNet, 2014. Disponível em: <https://www.zdnet.com/article/25-billion-connected-devices-by-2020-to-build-the-internet-of-things/>. Acesso em: 07 jan. 2021.

BARTOLINI, C.; MUTHURI, R.; SANTOS, C. Using ontologies to model data protection requirements in workflows. *In*: Otake M., Kurahashi S., Ota Y., Satoh K., Bekki D. **New Frontiers in Artificial Intelligence**. v. 10091. Cham: Springer, 2017.

BIONI, B. R. Compreendendo o conceito de anonimização e dado anonimizado. **Revista do Advogado AASP**, São Paulo, n. 144, p. 23-31, nov. 2019.

BMA. **Guidance note**: template data sharing agreement and data processing agreement. 2019. London: British Medical Association, 2019. Disponível em: <https://www.bma.org.uk/media/1491/bma-data-sharing-guidance-aug-2019.pdf>. Acesso em: 02 maio 2020.

BOFF, S. O.; FORTES, V. B. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência**, Florianópolis, n. 68, jan./jun. 2014. Disponível em: <https://www.scielo.br/pdf/seq/n68/06.pdf>. Acesso em: 02 jun. 2020.

BONATTI, P. *et al.* Transparent personal data processing: the road ahead. *In: International Conference on Computer Safety, Reliability, and Security, Lecture notes in computer science*, Sept. 2017. Doi: 10.1007/978-3-319-66284-8_28. Disponível em: <https://www.specialprivacy.eu/images/documents/TELERISE17.pdf>. Acesso em: 8 jan. 2021.

BRAMAN, S. Information policy and power in the information state. *In: BRAMAN, S. Change of state: Information, policy, and power.* Massachusetts: MIT Press, 2006. p. 313-328. Disponível em: http://people.tamu.edu/~braman/bramanpdfs/028_Braman_Chapt9.pdf. Acesso em: 02 jun. 2020.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 jun. 2020.

BRUNO, F. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade.** Porto Alegre: Sulina, 2013. Disponível em: <https://comunicacaoeidentidades.files.wordpress.com/2014/07/pg-18-a-51-maquinas-de-ver-modos-de-ser.pdf>. Acesso em: 02 jun. 2020.

BUTERIN, V. **A next generation smart contract & decentralized application platform.** Ethereum White paper. 2013. Disponível em: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Acesso em: 02 jun. 2020.

CADWALLADR, C.; GRAHAM-HARRISON, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian**. 2018. Disponível em: <http://freestudio21.com/wp-content/uploads/2018/04/50-million-fb-profiles-harvested-by-cambridge-analitica.pdf>. Acesso em: 02 jun. 2020.

CASTRO, F. G.; SABBAG, D. M. A.; DANTAS, P. R. G. **O acesso à informação e assimetrias informacionais no Brasil: um estudo preliminar.** FEBAB, v. 27, 2017. Disponível em: <https://portal.febab.org.br/anais/article/view/1719/1720>. Acesso em: 02 maio 2020.

CHA, S. C. *et al.* **A blockchain connected gateway for BLE-based devices in the internet of things.** IEEE Access, pp. 1-1, 2018.

CHUEN, L. **Investigating apps that share personal data to Facebook without user consent.** 2019. Disponível em: <https://responsibledata.io/2019/07/16/investigating-apps-that-share-personal-data-to-facebook-without-user-consent/>. Acesso em: 20 jul. 2020.

CNIL. **Transmission des données à des partenaires à des fins de prospection électronique**: quels sont les principes à respecter? CNIL, 28 dez. 2018. Disponível em: <https://www.cnil.fr/fr/transmission-des-donnees-des-partenaires-des-fins-de-prospection-electronique-quels-sont-les>. Acesso em: 02 jun. 2020.

COMISSÃO EUROPEIA. **O que são dados pessoais?** 2020a. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. Acesso em: 10 jul. 2020.

COMISSÃO EUROPEIA. **O que é um responsável pelo tratamento ou um subcontratante?** 2020b. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_pt. Acesso em: 10 jul. 2020.

CRUZ, J. C. Tecnologia Blockchain: um novo paradigma no ciclo de vida dos dados. *In: Workshop de Informação, Dados e Tecnologia*, 2., 2018, João Pessoa. **Anais [...]**. João Pessoa: UFPB, 2018. p. 588-598. Disponível em: https://dadosabertos.info/enhanced_publications/idt/enhanced_papers/27.pdf. Acesso em: 7 jan. 2021.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento empresarial**. Rio de Janeiro: Campus, 1998.

DE FILIPPI, P. The interplay between decentralization and privacy: the case of blockchain technologies. **Journal of Peer Production**, Paris, n. 7, p. 1-19, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689. Acesso em: 20 jul. 2020.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>. Acesso em: 5 jan. 2021.

DONEDA, D. A. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DUMBILL, E. **What is big data?** an introduction to the big data landscape. O'Reilly, 2012. *Online*. Disponível em: http://radar.oreilly.com/2012/01/what-is-big-data.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+oreilly%2Fradar%2Fatom+%28O%27Reilly+Radar%29. Acesso em: 10 jun. 2020.

EICHLER, N. *et al.* **Blockchain, data protection, and the GDPR**. Blockchain Bundesverband. 2018. Disponível em: https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Acesso em: 10 jul. 2020.

FABIANO, N. **Blockchain and data protection**: the value of personal data. Nicfab. 2018. Disponível em: <https://www.nicfab.it/blockchain-data-protection/>. Acesso em: 10 jul. 2020.

FACEBOOK. Política de dados. 2020. Disponível em: <https://www.facebook.com/privacy/explanation>. Acesso em: 10 jul. 2020.

FEDERAL TRADE COMMISSION. **Internet of things: privacy & security in a connected world**. Jan. 2015. Disponível em: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>. Acesso em: 07 jan. 2021.

FERREIRA, J. E. **Blockchain para criação de novos modelos de negócio e seus impactos na indústria de serviços financeiros**. 2017. Orientador: José Carlos Cavalcanti. Trabalho de Conclusão de Curso (graduação em Sistemas de Informação) – Universidade Federal de Pernambuco, Centro de Informática, 2017. Disponível em: <https://www.cin.ufpe.br/~tg/2017-1/jef-tg.pdf>. Acesso em: 02 jun. 2020.

FILIPPONE, R. **Blockchain and individuals' control over personal data in European data protection law**. Tilburg University, 2017. Disponível em: <https://pdfs.semanticscholar.org/2936/dbec731657e1cc5c10291f08a6c85e2ab1f6.pdf>. Acesso em: 10 jul. 2020.

FORMIGONI, J. R.; BRAGA, A. M.; LEAL, R. L. V. **Tecnologia Blockchain: uma visão geral**. 2017. Disponível em: <https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf>. Acesso em: 02 jun. 2020.

GDPR General Data Protection Regulation. **REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho** (General Data Protection Regulation). 2016. Disponível em: <https://www.privacy-regulation.eu/pt/index.htm>. Acesso em: 10 jul. 2020.

GEELKERKEN, F.W.J.; KONINGS, K. **Using blockchain to strengthen the rights granted through the GDPR**. Aphd, 2017. Disponível em: <http://aphd.ua/publication-353/>. Acesso em: 10 jul. 2020.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GOOGLE. **Política de Privacidade**. 2020. Disponível em: <https://policies.google.com/privacy>. Acesso em: 10 jul. 2020.

GREAVES, P.; NAUWELAERTS, W. **UK ICO publishes new data sharing code**. Alston & Bird Privacy, cyber & data strategy blog. 21 dez. 2020. Disponível em: <https://www.alstonprivacy.com/uk-ico-publishes-new-data-sharing-code/?cn-reloaded=1>. Acesso em: 5 jan. 2021.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29.º. **Parecer 05/2014 sobre técnicas de anonimização**: adotado em 10 de abril de 2014. 2014. Disponível em: <https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf>. Acesso em: 10 jul. 2020.

GRUPO DE TRABALHO DO ARTIGO 29.º SOBRE A PROTECÇÃO DE DADOS. **Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante**. fev.

2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_pt.pdf. Acesso em: 10 jul. 2020.

HEUKELOM, S.; NAVES, J.; VAN GRAAFEILAND, M. **Whitepaper juridische aspecten van blockchai**. Laatste versie bijgewerkt, 2017. Disponível em: https://www.platformoutsourcing.nl/f/files/download/overig/whitepaper_blockchain.pdf. Acesso em: 10 jul. 2020.

HIGA, P. **267 milhões de dados de perfis do Facebook são vendidos por US\$ 600**. Tecnoblog, 21 abr. 2020. Disponível em: <https://tecnoblog.net/335113/267-milhoes-perfis-facebook-sao-vendidos-na-dark-web/>. Acesso em: 10 jul. 2020.

ICO. **Annex B: Data sharing request form template**. 2020b. Disponível em: <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/annex-b-data-sharing-request-form-template/>. Acesso em: 8 jan. 2021.

ICO. **Annex A: Data sharing checklist**. 2020d. Disponível em: <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/>. Acesso em: 7 jan. 2021.

ICO. **Data sharing code of practice**. Information Commissioner's Office, dez. 2020a. Disponível em: <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/annex-a-data-sharing-checklist/>. Acesso em: 02 jun. 2020.

ICO. **Data sharing code of practice: draft code for consultation**. Information Commissioner's Office, jul. 2019. Disponível em: <https://ico.org.uk/media/for-organisations/data-sharing-a-code-of-practice-1-0.pdf>. Acesso em: 02 jun. 2020.

ICO. **Data sharing decision form template**. 2020c. Disponível em: <https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/annex-b-data-sharing-request-form-template/data-sharing-decision-form-template/>. Acesso em: 8 jan. 2021.

ISAAK, J.; HANNA, M. J. **User data privacy: Facebook, Cambridge Analytica, and privacy protection**. The Policy Corner, ago. 2018. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400>. Acesso em: 02 jun. 2020.

JENSEN, M. C.; MECKLING, W. H. Theory of the firm: managerial behavior, agency costs and ownership structure. **Journal of Financial Economics**, 1976. Disponível em: [https://josephmahoney.web.illinois.edu/BA549_Fall%202012/Session%205/5_Jensen_Meckling%20\(1976\).pdf](https://josephmahoney.web.illinois.edu/BA549_Fall%202012/Session%205/5_Jensen_Meckling%20(1976).pdf). Acesso em: 02 jun. 2020.

KITCHENHAM, B. **Procedures for performing systematic reviews: joint technical report**. Keele: Keele University, 2004.

LGPD: 85% das empresas ignoram questionamentos sobre tratamento de dados. Convergência digital, 01 dez. 2020. Disponível em: <https://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=55622&sid=5>. Acesso em: 11 jan. 2021.

LIMA, R. B. L.; SANTOS, P. L.; SANTARÉM SEGUNDO, J. E. Padrão de metadados no domínio museológico. Scielo, **Perspectivas em Ciência da Informação**, v. 21, n. 3, p. 50-69, jul./set. 2016. Disponível em: <https://www.scielo.br/pdf/pci/v21n3/1981-5344-pci-21-03-00050.pdf>. Acesso em: 02 jun. 2020.

LOTT, Y. M.; CIANCONI, R. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. Scielo, **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 23, n. 4, out/dez. 2018. Disponível em: https://www.scielo.br/scielo.php?script=sci_abstract&pid=S1413-99362018000400117&lng=en&nrm=iso&tlng=pt. Acesso em: 02 de jun. 2020.

LUCERO, S. **IoT platforms: enabling the Internet of Things**. White paper, IHS Technology. 2016. Disponível em: <https://cdn.ihs.com/www/pdf/enabling-IOT.pdf>. Acesso em: 10 jul. 2020.

MAGRANI, E.; OLIVEIRA, R. M. A internet das coisas e a Lei Geral de Proteção de Dados: reflexão sobre os desafios do consentimento e do direito à explicação. **Revista do Advogado**, AASP, São Paulo, v. 144, p. 80-89, nov. 2019.

MARTINS, P. B. L. **Dados pessoais sensíveis e inferências**. DTIBR, 18 maio 2019. Disponível em: <https://www.dtibr.com/post/dados-pessoais-sens%C3%ADveis-e-infer%C3%A2ncias>. Acesso em: 7 jan. 2021.

MASON, R. O. Four ethical issues of the information age. **MIS Quarterly**, v. 10, n. 1, p. 5-12, 1986.

MAYER-SCHÖNBERGER, A. V. **Delete: the virtue of forgetting in the digital age**. Princeton University Press, 2011.

MELHORES PRÁTICAS PARA DADOS NA WEB: forneça metadados.W3C Brasil blog, 30 maio 2016. Disponível em: <https://blog.w3c.br/forneca-metadados/>. Acesso em: 02 jun. 2020.

MILLER, S. **Metadata for digital collection: a how-to-do-it manual**. New York; London: Neal-Schuman, 2004.

MPDFT obtém decisão que suspende a venda de dados pessoais pela Serasa Experian. Ministério Público do Distrito Federal e Territórios, 23 nov. 2020. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12586-mpdft-obtem-decisao-que-suspende-a-venda-de-dados-pessoais-pela-serasa-experian> Acesso em: 11 jan. 2021.

NAKAMOTO, S. **Bitcoin: a peer-to-peer electronic cash system**. Bitcoin. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 10 jul. 2020.

NEISSEL, R.; STERI, G.; NAI-FOVINO, I. **A blockchain-based approach for data accountability and provenance tracking**. 2017. Disponível em: https://www.researchgate.net/publication/319047604_A_Blockchain-

based_Approach_for_Data_Accountability_and_Provenance_Tracking. Acesso em: 10 jul. 2020.

NISO. **Understanding metadata**: what is metadata, and what is it for? National Information Standards Organization, 2017. Disponível em: <https://www.niso.org/publications/understanding-metadata-2017>. Acesso em: 20 jul. 2020.

NUNES, A. C. **Dados são o petróleo da atualidade, diz futurista**. Época Negócios, jun. 2018. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/06/dados-sao-o-petroleo-da-atualidade-diz-futurista.html>. Acesso em: 02 jun. 2020.

PDPC. **Guide to data sharing**. Personal Data Protection Commission Singapore, 2018. Disponível em: https://iapp.org/media/pdf/resource_center/Guide_to_Data_Sharing.pdf. Acesso em: 02 jun. 2020.

PDPC. **Trusted data sharing framework**. Personal Data Protection Commission Singapore; IMDA, 2019. Disponível em: <https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf?page=50&zoom=100,-416,538>. Acesso em: 02 mai. 2020.

PARISER, E. **The filter bubble**: what the Internet is hiding from you. New York: Penguin Press, 2011.

PRASER, A. L. Vazamento de dados de pacientes com Covid-19 foi falha de funcionário: Ministério da Saúde rastreia possíveis divulgações das informações. **Radioagência Nacional**, 26 nov. 2020. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2020-11/vazamento-de-dados-de-pacientes-com-covid-19-foi-falha-de-funcionario>. Acesso em: 11 jan. 2021.

RANTOS, K. *et al.* Blockchain-based consents management for personal data processing in the IoT ecosystem. *In: International Joint Conference on e-Business and Telecommunications – ICETE (15., 2018). Proceedings [...]*, v. 2, p. 572-577. 2018. Disponível em: <http://utopia.duth.gr/~kdemertz/papers/SECRYPT.pdf>. Acesso em: 02 maio 2020.

SALMENSUU, C. **The General Data Protection Regulation and the blockchains**. Liikejuridiikka, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143992. Acesso em: 10 jul. 2020.

SAMSUNG. **Política de privacidade**. 2020. Disponível em: <https://www.samsung.com/br/info/privacy/>. Acesso em: 10 jul. 2020.

SANT'ANA, R. C. G. Cielo de vida dos dados e o papel da Ciência da Informação. *In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO*, 14., 2013, Florianópolis. Anais... Florianópolis, 2013. Disponível em: <http://200.20.0.78/repositorios/bitstream/handle/123456789/2477/CICLO%20DE%20VIDA%20DOS%20DADOS.pdf?sequence=1>. Acesso em: 5 jun. 2020.

SANT'ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da Ciência da Informação. **Informação & Informação**, Londrina, v. 21, n. 2, p. 116-142, maio/ago., 2016. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/download/27940/20124>. Acesso em: 10 jul. 2020.

SATER, S. Blockchain and the European Union's General Data Protection Regulation: a chance to harmonize international data flows. **SSRN Electronic Journal**, 2017. Disponível em: https://www.researchgate.net/publication/323979226_Blockchain_and_the_European_Union%27s_General_Data_Protection_Regulation_A_Chance_to_Harmonize_International_Data_Flows. Acesso em: 10 jul. 2020.

SCHWERIN, S. Blockchain and privacy protection in the case of the European General Data Protection Regulation (GDPR): A Delphi study. **The Journal of British Blockchain Association**, v. 1, n. 1, p. 1-77, 2018. Disponível em: https://www.researchgate.net/publication/326188512_Blockchain_and_Privacy_Protection_in_the_Case_of_the_European_General_Data_Protection_Regulation_GDPR_A_Delphi_Study. Acesso em: 10 jul. 2020.

SETZER, V. Dado, informação, conhecimento e competência. **DataGramZero: Revista de Ciência da Informação**, Rio de Janeiro, n. 0, dez., 1999. Disponível em: <https://brapci.inf.br/index.php/res/download/45629>. Acesso em: 07 jan. 2021.

SILVEIRA, S. A.; AVELINO, R.; SOUZA, J. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 217-230, nov. 2016. Disponível em: <http://revista.ibict.br/liinc/article/view/3719/3138>. Acesso em: 10 jul. 2020.

SINGAPURA STATUS ONLINE. **Personal data protection Act 2012**: No. 26 of 2012. Government Gazette: Acts Supplement, n. 25, 2012. Disponível em: <https://sso.agc.gov.sg/Act/PDPA2012>. Acesso em: 7 jan. 2021.

STRAVA. **Política de privacidade**. Disponível em: <https://www.strava.com/legal/privacy?hl=pt-BR>. Acesso em: 10 jul. 2020.

SWANSON, T. **Consensus as a service**: a brief report on the emergence of permissioned, distributed ledger systems. 2015. Disponível em: <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>. Acesso em: 10 jul. 2020.

SZABO, N. **The idea of smart contracts**. 1997. Disponível em: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html#:~:text=Smart%20contracts%20go%20beyond%20the,and%20controlled%20by%20digital%20means.&text=The%20smart%20contract%20design%20strategy,terms%20which%20deal%20with%20it>. Acesso em: 02 jun. 2020.

TAVANI, H. T. Informational privacy: concepts, theories, and controversies. *In*: HIMMA, K. E.; TAVANI, H. T. (Ed.). **The handbook of information and computer ethics**. New Jersey: John Wiley & Sons, 2008.

TRUONG, N. B. *et al.* Compliant personal data management: a blockchain-based solution. Cornell University. **IEEE Transaction in Information Forensics and Security**, 2019. DOI: 10.1109/TIFS.2019.2903659. Disponível em: <https://arxiv.org/abs/1904.03038>. Acesso em: 02 jun. 2020.

UNESCO. **O programa de Comunicação e Informação**. [Brasília], 2015. Disponível em: <http://unesdoc.unesco.org/images/0023/002321/232157por.pdf>. Acesso em: 02 maio 2020.

UNESP. **Programa de Pós-Graduação em Ciência da Informação**. Marília, 2019. Disponível em: <https://www.marilia.unesp.br/Home/Pos-Graduacao/CienciadaInformacao/ppgci.pdf>. Acesso em: 20 jul. 2020.

UNESP. **Programa de Pós-Graduação em Ciência da Informação (PPGCI)**. 2020. Disponível em: <https://www.marilia.unesp.br/#!/posci>. Acesso em: 25 jun. 2020.

WACHTER, S.; MITTELSTADT, B. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. **Columbia Business Law Review**, n. 2, out. 2019. Disponível em: <https://ssrn.com/abstract=3248829>. Acesso em: 07 jan. 2021.

WEF. **Personal data**: the emergence of a new asset class. World Economic Forum, May, 2011. Disponível em: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. Acesso em: 20 jul. 2020.

WHATSAPP. **Política de privacidade**. 2020. Disponível em: https://www.whatsapp.com/privacy/?lang=pt_br. Acesso em: 10 jul. 2020.

ZYSKIND, G.; OZ, N.; PENTLAND, A. S. Decentralizing privacy: using blockchain to protect personal data. **IEEE**, 2015. Disponível em: <https://ieeexplore.ieee.org/document/7163223>. Acesso em: 02 jun. 2020.