Revista Brasileira de
Risco e Seguro

A Privacidade de Dados no Open Insurance

Luíza Neves Marques da Fonseca
Doutoranda em Administração de Empresas – IAG, PUC-Rio. Bacharel em Relações Internacionais pela Universidade Federal Fluminense (2016), mestre em Administração de Empresas pela PUC-Rio (2019), atualmente cursando doutorado em Administração de Empresas na mesma instituição. Possui experiência na área de Conduta de Mercado e Relações com Consumidor na Confederação Nacional das Seguradoras (CNSeg) e atualmente presta consultorias para internacionalização de empresas para a Apex-Brasil e CNX Global.
luizaneves@phd.iag.puc-rio.br

Bernardo Graciolli Moreira Barroso
Bacharel em Relações Internacionais pela Universidade Federal Fluminense (2015). Possui MBA em Gestão de Seguros e Resseguro pela Escola de Negócios e Seguros (2018), e atua no setor de seguros há quase dez anos, onde se especializou em Gestão ASG. É certificado pelo CFA Institute no módulo ESG Investing e possui o CESGA (Certified ESG Analyst), emitido pela EFFAS.
graciollibernardo@hotmail.com

Resumo

Este artigo se propôs a incluir o ponto de vista do consumidor na discussão sobre a privacidade de dados no ambiente de Open Insurance, averiguando a sua disponibilidade de vir a compartilhar suas informações com empresas seguradoras no Brasil futuramente. Para tal, utilizou-se como método múltiplos casos de estudo, conduzidos através de entrevistas semi-estruturadas com potenciais consumidores do serviço. O estudo buscou estabelecer uma relação entre os antecedentes quanto a exposição de dados online e os benefícios potenciais esperados pelos consumidores com a sua propensão a aderir a esse novo ecossistema. Ademais, verificou-se se a Lei Geral de Proteção de Dados (LGPD) poderia contribuir para aumentar a confiança do consumidor frente a tal questão. Dessa forma, pôde-se contribuir com a incipiente literatura sobre o tema do Open Insurance, bem como com agentes do mercado segurador envolvidosno processo de inovação e criação do OI no Brasil.

Palavras-chave

Open Insurance; privacidade de dados; confiança do consumidor; LGPD.

Sumário

1. Introdução

A era da informação transformou a forma como os negócios são conduzidos nas mais diversas indústrias. O acesso ao *Big Data* – informações provenientes de mídias sociais, tráfego online, smartphones e tablets, *machine data* etc. – e a habilidade de agregar e analisar esses dados pode ser considerada hoje uma grande vantagem competitiva para empresas, uma tendência rumo a se acentuar (ERNST & YOUNG, 2014). Essa realidade não poderia ser diferente para uma indústria cujos fundamentos estão ligados à análise de dados: a seguradora. A contratação do seguro envolve a disponibilização de uma enorme quantidade de informações pessoais por parte do segurado (AWREY; MACEY, 2022). A partir dessas informações, utilizando-se tecnologias de análise de dados e predição de comportamento, as seguradoras poderiam melhor identificar os perfis de seus clientes e ofertar serviços personalizados, aderentes às suas necessidades. O desenvolvimento do Open Insurance (OI) já é uma realidade no mundo e no Brasil, onde as operações estão previstas para começar em 2023[1]. Contudo, a produção acadêmica sobre o tema ainda é considerada incipiente (STANDAERT; MUYLLE, 2022).

Por enquanto, as discussões sobre OI estão restritas ao mercado segurador e seus reguladores, e pouco se sabe sobre o ponto de vista do consumidor em relação a essas mudanças. Espera-se que o estabelecimento do OI fomente a competição, a inovação e a agilidade da área em responder às demandas de seus clientes, o que traria melhorias para os consumidores relacionadas ao acesso, ofertas, personalização de produtos/serviços, além de aumentar o controle dos consumidores sobre a utilização de seus dados. Por outro lado, o compartilhamento de informações necessário para viabilizar o OI aumenta os riscos de vazamento de dados, mau uso e fraude (EIOPA, 2021). Em se tratando de dados sensíveis que podem abranger até mesmo a situação financeira, de saúde e localização do segurado, o sentimento de insegurança do consumidor pode ser exacerbado.

Sabendo que a decisão sobre compartilhamento online de dados com empresas nem sempre segue uma lógica racional de custo/benefício (FERNANDES; PEREIRA, 2021), o presente estudo buscou entender como o consumidor enxerga as possibilidades que vão advir com o OI, e a sua disponibilidade para participar desse ecossistema autorizando tal compartilhamento dados pessoais em diferentes níveis, conforme previsto por Standaert e Muylle (2022). Através de entrevistas em profundidade, procurou-se averiguar a relação dos antecedentes e benefícios esperados por potenciais consumidores do OI com o seu grau de pretensão de aderir a esse novo ecossistema no futuro próximo. Ademais, o estudo buscou verificar se a Lei Geral de Proteção de Dados (LGPD) e o controle concedido ao indivíduo sobre a partilha de seus dados exercem algum tipo de influência nessa relação, contribuindo para aumentar sua confiança frente a tal questão.

[1] Fonte: Susep (2022).

2. Referencial Teórico

2.1 Open Insurance e a LGPD

O conceito de OI, sua definição e limites ainda estão sendo desenvolvidos pela Academia, autoridades de supervisão e partes envolvidas. No Brasil, o ambiente de OI ou Sistema de Seguros Aberto foi proposto pelo Conselho Nacional de Seguros Privados por meio da Resolução CNSP nº 415, de 20 de julho de 2021, que define o OP como "*compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas no* âmbito *dos mercados de seguros, previdência complementar aberta e capitalização*".

Um conceito equivalente e mais aprofundado é o de *open finance,* estrutura de compartilhamento de dados por instituições financeiras que possui premissas equivalentes com o OI, apesar de o modelo de negócios de uma seguradora ser diferente de outras instituições financeiras (THIMANN, 2014). A estrutura dos modelos abertos de compartilhamento de dados de instituições financeiras possui três princípios: acesso, portabilidade e interoperabilidade, ou seja, dados cedidos com o consentimento do segurado devem ser livres de acesso às instituições autorizadas por ele, ser transitáveis entre sistemas e estarem em uma linguagem comum (STANDAERT; MUYLLE, 2022).

Aos três requisitos para o ambiente aberto, soma-se um outro conceito fundamental: o de propriedade sobre os dados. Legislações e regulações de distintas jurisdições são inequívocas ao expressar que as informações financeiras são de propriedade dos consumidores que, portanto, têm o direito de agregar, deletar ou vender suas informações, independente de autorização ou consentimento da instituição com a qual tenham feito negócio (FRACASSI; MAGNUSON, 2021). No Brasil, o referencial para a proteção de dados é a Lei nº 13.709, de 14 de agosto de 2018, ou LGPD. A legislação reafirma a observância de garantias do art. 5º da Constituição Federal ao tratamento de dados digitais, como o direito à intimidade, o direito à liberdade de expressão, a inviolabilidade da intimidade, da vida privada das pessoas e do sigilo da correspondência (FEIJÓ, 2019).

Para tanto, o legislador introduziu dez princípios que devem orientar o tratamento de dados em território nacional: de finalidade, em que os propósitos legítimos devem ser informados e consentidos pelo titular dos dados; adequação, que garante a compatibilidade do tratamento de dados com a finalidade informada; necessidade, que limita o tratamento ao mínimo necessário para sua finalidade; livre acesso, para dar aos titulares facilidade de acesso às suas próprias informações; qualidade dos dados, para assegurar sua clareza, relevância e atualização; segurança, conferindo medidas técnicas para evitar seu uso indevido; prevenção, que dispõe sobre a utilização de medidas preventivas contra o "vazamento" de dados; não discriminação, proibindo o uso de dados para objetivos discriminatórios e, por fim, responsabilização e prestação de contas, para a transparência dos meios disponíveis pelo agente tratador de dados da eficácia de seu sistema de proteção e prevenção a vazamentos.

2.2 Privacidade, Confiança e Vulnerabilidade do Consumidor

A teoria de gestão de comunicação e privacidade acredita que existe uma relação transacional no gerenciamento de informações privadas, cujo "limite" se afina ou alarga conforme a disposição das pessoas em compartilhar mais ou menos informações (PETRONIO, 2002). Essa decisão pessoal pode se basear em um *trade-off* entre os benefícios percebidos e custos esperados com a perda de privacidade (CULNAN; ARMSTRONG, 1999). Os riscos associados à quebra de privacidade online possuem diferentes graus de gravidade, variando desde o recebimento de propagandas indesejadas, venda de dados pessoais para terceiros sem o consentimento do consumidor e instalação de dispositivos para monitorar as atividades online, até o vazamento de informações devido a falhas na segurança, que culminam em tentativas de fraudes e golpes. Em contrapartida, os benefícios podem ser de natureza monetária ou não, em forma de descontos, serviços personalizados, conveniências etc. (PRINCE, 2018).

Contudo, a literatura indica que decisões do consumidor sobre sua privacidade não são inteiramente explicadas por aspectos tão racionais quanto um cálculo de custos e benefícios, principalmente quando esse consumidor pode não estar ciente de todos os riscos, ou de como mitigá-los. Portanto, essas escolhas também contam com alguns aspectos irracionais e contextuais (FERNANDES; PEREIRA, 2021). O "paradoxo da privacidade" aponta que, embora indivíduos declarem possuir altas intenções de proteger sua privacidade, o seu comportamento online em relação aos dados pessoais tende a indicar o contrário (BARTH; DE JONG, 2017). De fato, o consumidor ordinário parece não entender completamente as implicações de sua privacidade, e não sente que possui controle suficiente para proteger seus dados (PILTON; FAILY; HENRIKSEN-BULMER, 2021).

Estudos reportam que confiar na empresa afeta a disposição dos consumidores de compartilhar informações online (DINEV; HART, 2006) e, por sua vez, a propensão a confiar é influenciada pelo nível de consciência sobre fraudes nos ambientes virtuais e suas experiências passadas envolvendo a Internet e situações de risco (TAN; THOEN, 2001). Os sentimentos negativos dos consumidores em relação ao uso de seus dados partem da ansiedade sobre o dano potencial, e não necessariamente de uma violação concreta ou má reputação da empresa, embora possa ser aguçada dessa forma (PALMATIER; MARTIN, 2019). Ao coletar, armazenar e analisar dados sobre seus consumidores, as empresas os colocam em posições de vulnerabilidade, mesmo que não haja nenhuma irregularidade ou dano.

3. Metodologia

O presente artigo utilizou casos de estudos múltiplos como metodologia, para obter um entendimento aprofundado sobre um fenômeno emergente: o surgimento do OI no Brasil e a possibilidade de os consumidores compartilharem seus dados e informações pessoais com seguradoras no futuro próximo (YIN, 1994).

Para seguir uma lógica de replicação, oito casos foram selecionados, com base em sua probabilidade de contribuir com *insights* para expandir o conhecimento sobre o tema e o problema de pesquisa, ajudando no avanço da construção teórica (EISENHARDT; GRABNER, 2007). Alguns dos critérios utilizados foram: i) indivíduos que já tomaram ou tomam constantemente decisões sobre aquisição de seguros; e ii) indivíduos que não atuam especificamente na área de seguros. Ademais, a seleção buscou um número equilibrado de homens e mulheres, abrangendo entrevistados de um amplo escopo de faixa etária (27-65 anos) e nível de escolaridade, de forma a garantir maior variabilidade de opiniões. Assim, os casos escolhidos envolvem indivíduos desfavoráveis, neutros e favoráveis à possibilidade de adesão ao OI, por diferentes motivos.

As entrevistas conduzidas seguiram um questionário semiestruturado, com o objetivo de guiar e elucidar a conversa sobre o tema. As questões formuladas tiveram como base a literatura existente e foram introduzidas em uma conversa geral sobre a relação do indivíduo com a sua privacidade na Internet e seus hábitos de gestão da privacidade online. Em seguida, realizou-se uma apresentação sobre o conceito de OI e as novas possibilidades de produtos e benefícios que podem advir a partir disso, para que os entrevistados pudessem opinar sobre que dados estariam dispostos a compartilhar, os benefícios esperados em troca e a sua confiança nos agentes envolvidos no processo. Por fim, deu-se uma breve introdução sobre a LGPD, seus mecanismos de controle, transparência e supervisão para gestão de dados pessoais, a fim de averiguar se a sua existência influencia a decisão dos consumidores sobre sua intenção de adesão ao OI. As entrevistas duraram, em média, 35 minutos, e foram transcritas para possibilitar a análise dos dados. As transcrições foram examinadas individualmente e amplamente discutidas entre os autores, com intuito de compará-las para identificar padrões repetidos, categorizações, dimensões e possíveis refutações (SPIGGLE, 1994).

4. Discussão dos Resultados

4.1 Antecedentes

Em relação aos antecedentes averiguados, buscou-se entender o grau de vulnerabilidade percebido pelo indivíduo em relação à exposição de seus dados online, visto que todos os entrevistados declararam utilizar a Internet para desempenhar as mais diversas atividades: lazer, comunicação, trabalho, estudo, compras, pagamentos e transferências bancárias, armazenamento de arquivos etc. O sentimento geral dos respondentes é de que estão sim, como usuários de diversos sites, aplicativos e redes online, em posição de vulnerabilidade no que tange à exposição dos seus dados pessoais e aos diversos fins para os quais estes podem ser utilizados por terceiros, e que não possuem controle sobre isso. Esse sentimento se origina em grande medida do desconhecimento sobre qual seria a extensão dos riscos a que tais consumidores estão expostos, conforme apontado por Pilton, Faily e Henriksen-Bulmer (2021), e pode chegar ao ponto de deixar de ser uma preocupação, pois acreditam que não têm escapatória, ou que não detêm o conhecimento e as ferramentas necessárias para lidar com a questão.

> "É o tipo de coisa que eu gosto de não pensar sobre. Não me incomoda porque eu não sei realmente o que pode ser feito com isso, então não me preocupo." (nº 5)

> "Controle eu não tenho, mas eu confio nas empresas. Eu também não sei o quanto de risco existe nisso. Eu me preocupo com dados bancários, essas coisas." (nº 2)

Segundo Barth e De Jong (2017), embora indivíduos declarem possuir altas intenções de proteger sua privacidade, o seu comportamento online em relação aos dados pessoais tende a indicar o contrário. As entrevistas realizadas vão ao encontro disso, pois ninguém relatou ser tão cuidadoso com seus dados pessoais quanto gostaria, mesmo os que disseram tomar cuidados em relação aos seus *logins* e senhas, políticas de privacidade dos sites, protocolos de dupla confirmação, uso de [impressão] digital ou reconhecimento facial para proteção de dispositivos e aplicativos, ou aplicativos de segurança para resguardar o acesso a e-mail e demais sites com informações sensíveis. Ressaltou-se a dificuldade de ler e compreender as políticas de privacidade, em que constam informações sobre quais dados serão coletados, os fins a que se destinam, se serão compartilhados com terceiros etc. Mais uma vez, esse sentimento da "incompreensão" faz com que a desconfiança na lisura do processo de guarda e análise de dados seja exacerbada.

> "Eu não me sinto tendo nenhum controle, e pode ser por ignorância, porque todos têm um termo de uso, contrato, mas eu confesso que toda vez que eu tento ler aquilo, desisto antes do final, porque não entendo nada." (nº 7)

Em relação ao nível de consciência dos entrevistados sobre situações de risco em geral que podem influenciar a confiança do consumidor e sua propensão a compartilhar dados (TAN; THOEN, 2001), todos estão cientes da ocorrência desses eventos, e alguns relataram acontecimentos pessoais de *phishing,* que consiste em enganar indivíduos para obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito, ou clonagem de números de celular etc., algo que pode se dar em decorrência de vazamentos de dados. Os respondentes também relataram que, após sofrerem ou presenciarem essas intercorrências, se tornaram mais conscientes dos riscos e passaram a ser mais cautelosos em relação à exposição de seus dados e ao uso dos aplicativos.

> "Também já aconteceu de entrarem em contato comigo fingindo ser a [*operadora de telefonia e Internet*], porque sabiam que eu tinha acabado de contratar o serviço e precisava realizar a instalação dos aparelhos na minha casa. Eles tinham informações minhas, meu endereço, por exemplo, e me pediam mais informações para proceder. Quando uma empresa com quem você está se relacionando vaza seus dados e alguém entra em contato, é muito mais arriscado. Eu quase acreditei que era mesmo a [*operadora*], porque eles já tinham muitas informações." (nº 2)

> "Já tive compras suspeitas no cartão de crédito. Eu tenho consciência que a gente que usa a Internet está suscetível a esse tipo de situação, então mantenho controle da minha fatura e quando vejo algo suspeito, entro em contato imediatamente com o banco. A partir dessas experiências a gente começa a usar mais as ferramentas de segurança." (nº 4)

4.2 Benefícios

Dentre os benefícios esperados pelos entrevistados por compartilhar seus dados no ambiente de OI, os mais citados foram obter descontos no seu seguro, preços mais acessíveis, a possibilidade de verificar o custo/benefício de diversas ofertas, facilitando a busca por um seguro, a personalização dos produtos de acordo com seus objetivos e necessidades e o recebimento de ofertas mais direcionadas.

> "Um seguro mais voltado para mim. Que perceba que nos últimos anos eu usei muito o reboque, mas nunca fui roubado, então me ofereça um seguro balanceado dessa forma." (nº 1)

> "Acho bom ter menos trabalho de pesquisa. Ter a possibilidade de um serviço mais personalizado e flexível para mim, sendo ofertado de forma mais fácil." (nº 2)

> "Se eles têm mais informações sobre mim, meus gostos e minha situação de vida, podem me ligar e oferecer serviços que façam sentido, melhores do que os que eu uso atualmente. Isso é melhor do que receber um monte de ligação oferecendo coisas que não me interessam." (nº 8)

Em contrapartida, alguns dos entrevistados que não têm pretensão de aderir a essa nova tecnologia não enxergam benefícios que os fariam mudar de ideia. Para a entrevistada nº 6, seria mais vantajoso compartilhar as informações desejadas individualmente com a seguradora de sua escolha em troca de possíveis benefícios do que a possibilidade de que todas tenham acesso em um ambiente compartilhado. Já para a entrevistada nº 7, alguns dados seriam sensíveis demais, não valendo a pena serem "trocados" por possíveis benefícios.

> "Não vejo benefício em permitir que todas elas tenham acesso a tudo. Se eu posso obter uma vantagem por meio disso, eu também posso obtê-la se eu procurar individualmente algumas seguradoras e passar essas informações eu mesma, não precisa ser [*uma troca*] entre elas." (nº 6)

> "Não me vem à cabeça nenhum benefício que faça a diferença. É mais uma questão de quais dados eu me importo de compartilhar ou não." (nº 7)

4.3 Cessão de dados e o papel da LGPD

Dentre os entrevistados que acreditam que não cederiam seus dados pessoais para um ambiente de seguros aberto, os principais motivos são não entenderem as consequências de ter informações expostas e não se considerarem uma pessoa que zele da melhor forma possível pela proteção desses dados; não terem interesse em obter os benefícios que poderiam ser oferecidos no ambiente de OI; ou não confiarem que seus dados estariam seguros e seriam usados apenas para os fins previamente acordados, devido a experiências passadas com empresas que não respeitaram esse direito. Para esses consumidores, nem mesmo a supervisão da Superintendência de Seguros Privados (Susep) ou as normas estabelecidas pela LGPD serviriam plenamente para garantir a integridade das suas informações.

> "Acho que eu não confiaria nesse modelo, porque já é difícil você conter essa informação quando a empresa só pode usar dentro dela, imagina se ela puder compartilhar com outras, a possibilidade de vazamento dessas informações sensíveis é muito maior. Pela minha experiência, as empresas que eu tive contato e solicitei que não fossem utilizados mais meus dados, isso não funcionou. Então não tenho confiança, mesmo com regulamentação." (nº 6)

> "Não existe informação segura. Não confio que está seguro, nem dentro de banco, seguradora, nenhum sistema. Colocou em um sistema, na nuvem, alguma coisa pode acontecer." (nº 7)

Mesmo os que foram favoráveis à adesão ao OI impuseram suas restrições ou condições. Para uns, existem alguns dados (como os de geolocalização, patrimônio e renda, histórico de saúde, em geral) que são mais sensíveis do que outros (demográficos, disponíveis em redes sociais dos usuários, tráfego online, monitoramento de hábitos de direção e saúde, por exemplo).

> "Conheço pessoas que não se incomodam com isso [*fornecer dados de geolocalização*], mas para mim é desconfortável. Mesmo que o Google já tenha essa informação minha 24h por dia, pelo meu celular." (nº 8).

> "Esses dados [*hábitos sobre exercícios físicos, coletados por um dispositivo externo*] eu acho que eu poderia, porque o que alguém poderia fazer com eles? Se fosse para alguém tentar me vender coisas relacionadas a isso, tudo bem. É uma intromissão aceitável." (nº 7)

Para outros, o aceite está condicionado à garantia de que seus dados estarão em um ambiente seguro, supervisionado, que serão utilizados somente para os fins previamente acordados, e que a qualquer momento o consumidor teria o direito de optar por cessar sua participação. Nesse sentido, após serem apresentados aos termos gerais da LGPD, alguns respondentes afirmaram que a existência da regulamentação seria um fator importante para aumentar sua confiança nesse processo.

> "Se eu tivesse essa confiança no sigilo dessa informação que eu estou fornecendo, e de que esses dados serão resguardados, eu teria interesse em aderir sim [*ao OI*]. Só de saber que existe essa lei, você fica mais tranquilo em relação a isso. Dá mais segurança, porque você tem o direito de reclamar, de contestar, de ser ressarcido se você for exposto." (nº 3)

Por fim, alguns entrevistados acreditam que a cessão ou não de seus dados pessoais às empresas está mais ligada ao fato de terem acesso ao produto, serviços ou a algum benefício específico que obterão no ato de adesão do que no fato de acreditarem ou não que seus dados serão resguardados, ou que os mecanismos da lei serão mais ou menos eficazes.

> "Eu entendo como um mal inevitável, uma contrapartida. A gente só tem acesso a tantas coisas de graça, redes sociais por exemplo, porque estamos vendendo nossos dados. Para participar disso, acabo precisando ceder meus dados. Para ter benefício e a facilidade de comprar online, confio meus dados aos sites." (nº 2)

> "Eu não sei até que ponto esses trâmites legais são eficazes, não sei se na prática isso realmente faz efeito. Mas eu não vejo problema em compartilhar certos dados, desde que o retorno seja realmente eficaz. Se eu achar que o benefício não valeu a pena, ou que meus dados estão sendo usados para outras coisas sem sentido, cancelo tudo." (nº 8)

5. Conclusão

Este artigo buscou se aprofundar sobre as possibilidades de compartilhamento de dados pessoais por parte de consumidores no ambiente de OI, com o intuito de somar à incipiente literatura sobre o tema, contribuindo também com agentes do mercado segurador envolvidos no processo de inovação e criação do OI no Brasil. Ao analisar i) a forma como o indivíduo se sente e se posiciona em relação à exposição de seus dados na Internet, ii) situações anteriores de vazamento ou mau uso das suas informações, iii) os possíveis objetivos e benefícios que poderiam interessá-los nessa troca e iv) a efetividade da LGPD como mecanismo de garantia da segurança dos dados, buscou-se identificar os aspectos racionais, não racionais e contextuais que influenciam na propensão e na decisão dos consumidores de aderir ao OI, destacando diferentes posicionamentos e destrinchando as motivações e justificativas mais comuns.

Outras preocupações pertinentes surgiram durante as entrevistas, mas não foram abordadas neste artigo devido à limitação de escopo e espaço. A primeira delas se refere à possibilidade de que, ao compartilhar certas informações “desfavoráveis”, o seguro se torne proibitivo para certos indivíduos que possuam, por exemplo, um histórico de saúde que aponte doenças crônicas. O segundo ponto se refere ao uso em massa de dados individuais com o objetivo de manipular opiniões e/ou estimular certos comportamentos, até que ponto os indivíduos estão conscientes disso, e se esse seria um caminho salutar para o futuro da humanidade. Dessa forma, seria interessante que estudos posteriores sobre a utilização de dados no contexto do OI pudessem se aprofundar nessas questões.

Sobre as limitações da pesquisa, destacam-se as inerentes ao método de investigação, que impossibilita generalizações estatísticas e o estabelecimento de correlações entre as variáveis – antecedentes, benefícios e o grau de permissividade, ou intenção de compartilhar informações. Ademais, por se tratar de uma pesquisa feita com base em suposições sobre o comportamento do consumidor, que ainda não se deparou de fato com a perspectiva de aderir às inovações provenientes do OI, sugere-se que o estudo seja replicado futuramente, conforme o avanço do tema se torne mais palpável para a sociedade.

6. Referências bibliográficas

AWREY, D.; MACEY, J. The Promise and Perils of Open Finance. **ECGI Working Paper Series in Law**, n.632, 2022.

BARTH, S.; DE JONG, M.D. The privacy paradox. Investigating discrepancies between expressed privacy concerns and actual online behavior. A systematic literature review. **Telematics and Informatics**, v. 34, n.7, p. 1038-1058, 2017.

CULNAN, M. J.; ARMSTRONG, P. K. Information privacy concerns, procedural fairness, and impersonal trust. An empirical investigation. **Org. Science**, v.10, n.1, p.104-115, 1999.

EIOPA. **Open insurance**: Accessing and sharing insurance-related data. Discussion paper. EIOPA: 2021.

EISENHARDT, K.M.; GRAEBNER, M.E. Theory building from cases. Opportunities and challenges. **Academy of Mgmt J**., v.50, n.1, p.25-32, 2007.

EY. Ernst & Young. **Big Data**. Changing the way businesses compete and operate. 2014. Disponível em: https://motamem.org/wp-content/uploads/2019/01/Big-data-applications-and- insights.pdf. Acesso em: mar. 2022.

FEIJÓ, L.S. **A titularidade de dados pessoais**: uma análise da aplicabilidade do regime jurídico da propriedade. 2019. Disponível em: https://lume.ufrgs.br/handle/10183/221420. Acesso em: mar. 2022.

FERNANDES, T.; PEREIRA, N. Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? Telematics and Informatics, v. 65, 2021. https://doi.org/10.1016/j.tele.2021.101717.

FRACASSI, C.; MAGNUSON, W. Data autonomy. **Vand. L. Rev**., v. 74, p. 327-383, 2021.

PALMATIER, R.; MARTIN, K.D. The Psychology of Consumer Privacy. **The Intelligent Marketer's Guide to Data Privacy**. Berlim: Springer, 2019. p. 21-41

PETRONIO, Sandra. **Boundaries of Privacy**: Dialectics of Disclosure. Albany: State University of New York Press, 2002.

PILTON, C.; FAILY, S.; HENRIKSEN-BULMER, J. Evaluating privacy-determining user privacy expectations on the web. **Computers & security**, v. 105, 2021. https://doi.org/10.1016/j.cose.2021.102241

PRINCE, C. Do consumers want to control their personal data? Empirical evidence. **Int. J. of Human-Computer Studies**, v. 110, p. 21-32, 2018.

SPIGGLE, S. Analysis and interpretation of qualitative data in consumer research. **Journal of consumer research**, v.21, n.3, p.491-503, 1994.

STANDAERT, W.; MUYLLE, S. Framework for open insurance strategy: insights from a European study. **The Geneva Papers on Risk and Insurance-Issues and Practice**, p.1-26, 2022.

SUSEP. Superintendência de Seguros Privados. **Open Insurance**. [2022]. Disponível em: https://openinsurance.susep.gov.br. Acesso em: 28 ago. 2022.

TAN, Y.; THOEN, W. **Toward a generic model of trust for electronic commerce**. Int. J. of Electronic Commerce, v. 5, n. 2, p. 61-74, 2001.

THIMANN, C. How Insurers Differ from Banks: A Primer in Systemic Regulation. **SRC Special Paper**, v.3, 2014.

YIN, R. K. Discovering the future of the case study. Method in evaluation research. **Evaluation practice**, v.15, n.3, p. 283-290, 1994.