VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

FREDERICO THALES DE ARAÚJO MARTOS

JÉSSICA AMANDA FACHIN

AIRES JOSE ROVER

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Aires Jose Rover; Frederico Thales de Araújo Martos; Jéssica Amanda Fachin – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 978-65-5648-745-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

O VI Encontro Virtual do CONPEDI, realizado em parceria com o Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" das Faculdades Londrina e a Faculdade de Direito de Franca (FDF), ocorreu nos dias 20, 21, 22, 23 e 24 de junho de 2023. O evento teve como temática central "Direito e Políticas Públicas na Era Digital". As discussões realizadas durante o encontro, tanto nas diversas abordagens tecnológicas como nos Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Direito, Governança e Novas Tecnologias I", no dia 23 de junho de 2023, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas destacam o aspecto humano da Inteligência Artificial, os desafios para a democracia e a aplicação do Direito no ciberespaço, bem como reflexões atuais e importantes sobre a regulação das plataformas digitais e as repercussões das novas tecnologias em diversas áreas da vida social.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Prof. Dr. Aires Jose Rover - Universidade Federal de Santa Catarina/SC

Profa. Dra. Jéssica Fachin - Faculdades Londrina/PR

Prof. Dr. Frederico Thales de Araújo Martos - Faculdade de Direito de Franca/SP e Universidade do Estado de Minas Gerais/MG

GESTÃO DE RISCO NO TRATAMENTO DE DADOS PESSOAIS: OS MARKETPLACES DE FOOD DELIVERY E OS DESAFIOS IMPOSTOS PELA LEI 13.709/2018

RISK MANAGEMENT IN THE PROCESSING OF PERSONAL DATA: THE FOOD DELIVERY MARKETPLACES AND THE CHALLENGES IMPOSED BY LAW 13,709/2018

Rosane Leal Da Silva [1]
João Antônio de Menezes Perobelli [2]

Resumo

A Lei Geral de Proteção de Dados determinou várias mudanças às organizações, que tiveram que adequar suas atividades de gestão, tratamento, operação e controle de dados pessoais à legislação, resultando em novos procedimentos internos para garantir maior segurança aos titulares dos dados. Devido à pandemia do COVID-19, o processo de digitalização de empresas acelerou, expandindo o mercado de marketplace's, especialmente os de food delivery, que registraram crescimento elevado no período, com consequente aumento de dados pessoais tratados. A verificação desse cenário originou o problema de pesquisa: que estratégias devem ser utilizadas pelo segmento do marketplace´s de food delivery para o enfrentamento dos riscos do tratamento de dados pessoais, minorando-se os casos de incidência de responsabilidade civil dos agentes de tratamento? Para responder ao problema foi utilizado o método de abordagem indutivo e procedimento monográfico. Concluiu-se que LGPD favorece empresas que possuam eficientes políticas de governança e compliance para proteção e tratamento de dados pessoais e, especialmente no setor dos marketplaces de food delivery, evidencia-se a necessidade de modelos que envolvam os processos e sistemas internos das empresas, abrangendo os demais agentes de tratamento, como restaurantes e entregadores. Essas medidas são de grande importância, porque todos os agentes de tratamento de dados pessoais devem estar adequados à LGPD, sob pena de responsabilidade civil solidária dos implicados.

Palavras-chave: Dados pessoais, Food delivery, Gestão de risco, Lei geral de proteção de dados brasileira, Marketplace

Abstract/Resumen/Résumé

The General Data Protection Law determined several changes to organizations, which had to adapt their activities of management, treatment, operation and control of personal data to the

[1] Doutora em Direito, Professora do Curso de Graduação e Mestrado em Direito da UFSM, Professora do Curso de Direito da Universidade Franciscana. E-mail: rolealdasilva@gmail.com

[2] Graduado em Administração de Empresas e em Direito, ambos pela Universidade Franciscana. E-mail: perobelli.joao@gmail.com

legislation, resulting in new internal procedures to guarantee greater security to data subjects. Due to the COVID-19 pandemic, the process of digitizing companies accelerated, expanding the market for marketplaces, especially those for food delivery, which registered high growth in the period, with a consequent increase in the number of personal data processed. The verification of this scenario gave rise to the research problem: what strategies should be used by the food delivery marketplace's segment to face the risks of processing personal data, reducing cases of civil liability of processing agents? To answer the problem, the inductive approach method and monographic procedure were used. It was concluded that LGPD favors companies that have efficient governance and compliance policies for the protection and processing of personal data and, especially in the food delivery marketplace sector, there is a need for models that involve the companies' internal processes and systems, covering the other treatment agents, such as restaurants and couriers. These measures are of great importance, because all personal data processing agents must comply with the LGPD, under penalty of joint and several civil liability of those involved.

Keywords/Palabras-claves/Mots-clés: Personal data, Food delivery, Risk management, Brazilian general data protection law, Marketplace

1 INTRODUÇÃO

O crescente desenvolvimento das Tecnologias de Informação e Comunicação (TIC) proporcionou sua intensa penetração em variadas áreas, tais como econômica, política, educacional e social. Essa expansão foi impulsionada pela melhoria na infraestrutura de comunicação, especialmente com a conexão via telefones móveis, uma das variáveis que elevou o número de internautas, acesso que se mostrou especialmente importante no período da Pandemia de COVID-19.

O isolamento social forçou a migração de muitos serviços para o ambiente digital, com impactos importantes na área do consumo. Ocorre que, ao lado da facilidade de adquirir bens e serviços com poucos *cliks*, os processos de compra *on-line* acarretam diversas e complexas operações de tratamento de dados pessoais, a ensejar novos deveres por parte dos fornecedores, especialmente diante da edição da Lei nº 13.709/2018 - Lei Geral De Proteção de Dados - (LGPD). Essa legislação, ainda que editada com certo atraso se comparado a outros países, sobretudo os europeus, colocou o Brasil no seleto grupo de Estados que evidenciam preocupação com os direitos dos titulares, tão vulneráveis em meio aos processos tecnológicos de coleta e tratamento de seus dados pessoais.

A vigência da LGPD impôs a adaptação de diversos setores empresariais e consequentemente, forçou a criação (ou revisão) de procedimentos internos para garantir a segurança de dados pessoais tratados pelos controladores, ou seja, pessoas físicas ou jurídicas que, com fins econômicos, processam dados pessoais de terceiros. Ao lado de deveres de conduta derivados da boa-fé objetiva, já previstos na Lei nº 8.078, de 1990 (CDC), a LGPD inova não só ao tratar especificamente da proteção de dados pessoais, como também ao ampliar a percepção dos riscos inerentes ao processamento, que devem ser monitorados e mitigados ao máximo pelos agentes responsáveis pelo seu tratamento.

Para dar conta do desafio de proteger os dados pessoais do titular, a Lei 13.709/2018 prevê desde procedimentos mais simples até a adoção de sistemas mais complexos de segurança, bem como incentiva medidas de boas práticas a serem adotadas pelos agentes de tratamento de dados pessoais, o que pode mitigar a responsabilidade dos agentes de tratamento. É sobre esse tema que se volta o estudo, cujo objetivo central é analisar a responsabilidade dos agentes de tratamento do segmento *marketplaces de food delivery* e as medidas que podem ser adotadas para prevenir ou mitigar os riscos.

A análise se justifica em razão do elevado número de dados pessoais tratados em cada operação, ao que se soma o expressivo crescimento durante a pandemia do COVID-19, quando

o comércio online no Brasil teve um crescimento acumulado de 122% no período de janeiro a novembro de 2020 em comparação com o mesmo período de 2019, movimentando mais de R$115,3 bilhões no período (FOLHA DE SÃO PAULO, 2020). Os *marketplaces de food delivery* fazem parte desta estatística de comércio online e também registraram altos níveis de crescimento, fator que merece atenção porque todo esse processo de compra *online* envolve tratamento de dados pessoais, compartilhados entre vários agentes, incluindo os entregadores.

Logo, quanto mais dados pessoais são tratados e compartilhados, maior é o risco da operação, o que remete ao seguinte problema de pesquisa: quais estratégias devem ser utilizadas pelo segmento do *marketplace's* de *food delivery* para o enfrentamento dos riscos do tratamento de dados pessoais, minorando-se os casos de incidência de responsabilidade civil dos agentes implicados? Este questionamento é enfrentado a partir do emprego do método de abordagem indutivo, pois a pesquisa partiu de enfoque específico desse segmento, eleito para exame pelo método de procedimento monográfico, que permite examinar os elementos caracterizadores dessa forma de atuação e os processos empregados pelos agentes de tratamento implicados. Tal enfoque foi complementado pela abordagem normativa e doutrinária do tratamento de dados pessoais, o que permite, num passo seguinte, compreender a espécie de responsabilidade aplicável aos agentes em caso de incidente de segurança com os dados pessoais para, a partir desse aporte, identificar medidas para prevenir ou mitigar os riscos.

2 MARKETPLACE'S E FOOD DELIVERY: COMPREENDENDO COMO FUNCIONA O SEGMENTO.

A compreensão do *marketplace* pressupõe que se considere o desenvolvimento da *internet,* pois essa forma de atuação empresarial depende essencialmente dessa tecnologia. Segundo Akhmadi e Pratolo (2021, p. 2), o desenvolvimento da tecnologia e o exponencial crescimento no número de usuários conduziram ao surgimento de novas formas de negociação e alavancaram atividades como as realizadas nos *marketplace*s, definidos como espaços virtuais que permitem transações entre vendedores e compradores (fornecedores e consumidores), de maneira facilitada e com redução de custos da operação. Para os autores,

> Marketplace, or in other terms, is called "exchange" or "hub" is a virtual location with facilities to allow transactions between sellers and buyers. The marketplace itself is a form of intermediation independent from both sellers and buyers [6]. Another definition of the marketplace is an information system network that facilitates sellers and buyers to exchange information, carry out transactions and other activities before the transaction occurs [19]. In simple terms, a marketplace refers to a market where

> many sellers and buyers make transactions. The marketplace manager is a service provider bringing together sellers and buyers and independent from both of them [20]. (AKHMADI; PRATOLO, 2021, p. 3)[1]

No mesmo sentido é a definição apresentada por Luca (2017), para quem m*arketplaces* são plataformas de comércio eletrônico que reúnem diversos vendedores/lojas em um único local (aplicativo ou *site*), facilitando transações entre o pólo consumidor e o fornecedor, pois normalmente tais plataformas dão origem a operações que não ocorreriam de outra forma (LUCA, 2017, p.77). Trata-se do modelo *Business to Consumer* (B2C), no qual as empresas ofertam seus serviços e produtos usando uma plataforma que vai aproximá-las dos seus consumidores[2], o que fez com que os *marketplaces* passassem a ter variado "catálogo", o que inclui o ramo de alimentação (bares, restaurantes, entre outros), objeto de análise neste trabalho. Tal expansão facilita a realização de pedidos pelos consumidores, o que é feito com menos esforço e de forma mais conveniente e rápida, dando origem ao conceito de *marketplace de food delivery* (SEE-KWONG, SOO-RYUE, SHIUN-YI, LILY, 2017).

Ao operarem dessa forma, os *marketplaces de food delivery* se apresentam como uma ferramenta responsável por romper barreiras de comunicação entre os restaurantes e os consumidores, que a partir de então possuem acesso a uma plataforma ágil e prática, se comparado às demais formas de consumir em restaurantes (ÇAVUŞOĞLU, 2012, p.50). Sua atuação transformou o processo de realização de pedidos no ramo de alimentação, acompanhando a rápida incorporação das TIC no cotidiano das pessoas (ÇAVUŞOĞLU, 2012, p.58), o que foi ainda mais intensificado com a ocorrência da pandemia do COVID-19. Tal incremento forçou as empresas a criarem métodos de proteção aos dados pessoais[3] tratados nos

---

[1] Em livre tradução: Marketplace, ou em outros termos, é chamado de "exchange" ou "hub" é um local virtual com facilidades para permitir transações entre vendedores e compradores. O mercado em si é uma forma de intermediação independente de vendedores e compradores [6]. Outra definição de mercado é uma rede de sistema de informação que facilita a troca de informações entre vendedores e compradores, realização de transações e outras atividades antes que a transação ocorra [19]. Em termos simples, um mercado refere-se a um mercado onde muitos vendedores e compradores fazem transações. O gestor de marketplace é um prestador de serviços que reúne vendedores e compradores e é independente de ambos [20].

[2] Existem diferentes modelos de negócios de plataformas, destacando-se cinco que usualmente são descritos na literatura sobre o tema: a) *Business to Business* (B2B), modelo de comércio no qual os principais atores que transacionam na venda de produtos ou oferta de serviços são empresas e demais entidades corporativas; b) *Business to Consumer* (B2C), no qual figuram uma empresa e um consumidor direto, modelo no qual as empresas ofertam seus serviços e produtos usando uma plataforma; c) *Business to Government* (B2G), modelo caracterizado pela presença de empresas e governo, em que este pode atuar como consumidor ou em processos de licitações e concorrências públicas realizadas por meio de plataformas; d) *Consumer to Consumer* (C2C), no qual consumidores negociam diretamente por meio de transações *on-line;* e) *Consumer to Business* (C2B), oposto do modelo B2C, neste caso os consumidores utilizam as plataformas para vender bens ou serviços às empresas (AKHMADI; PRATOLO, 2021, p.4).

[3] Segundo a redação do art. 5º I, dado pessoal é descrito como toda informação relacionada a pessoa natural identificada ou identificável e, além dessa definição geral, há uma categoria que enseja maior proteção, denominada de dado pessoal sensível, definida no inciso II como "dado pessoal sobre origem racial ou étnica,

procedimentos cotidianos, isso porque o mercado opera em diferentes frentes e com o auxílio de operadores[4], isto é, outras empresas que atuam em conjunto e que são responsáveis por procedimentos específicos, como a realização do pagamento e a entrega dos pedidos.

Ao analisar especificamente esse modelo de negócios, percebe-se que os fluxos de dados pessoais ocorrem em diversas etapas no processo de compra no setor de *marketplaces* de *food delivery* e, em determinados momentos, os dados serão disponibilizados a terceiros, conforme verifica-se na imagem 1, abaixo.

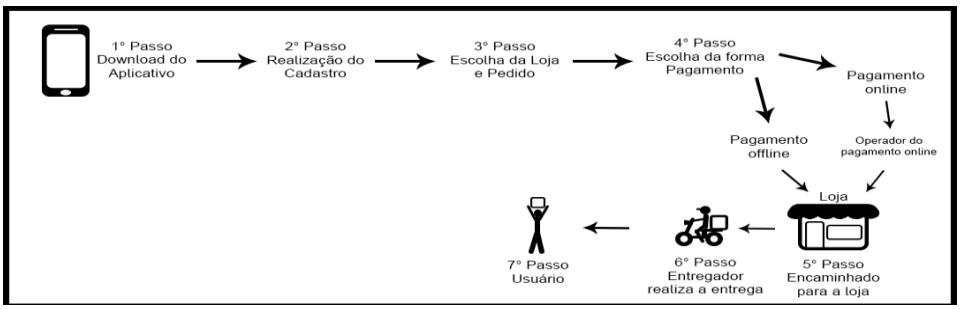

Imagem 1 – Tráfego de dados pessoais no processo de compra do usuário em *Marketplace's* de *food delivery* (AUTORES, 2022)

O primeiro passo que o usuário realiza para utilizar do *marketplace* é fazer o *download* do aplicativo. Concluído esse passo inicial, para conseguir realizar sua compra ou pedido o usuário precisa efetuar o cadastro, momento no qual fornece seu nome completo, número de CPF, e-mail, número do telefone, endereço, localização e data de nascimento. Em conjunto com tais dados o aplicativo já coleta, de forma automática, informações sobre o modelo do *smartphone* e seu sistema operacional[5].

A partir de então o *marketplace* já terá todas as informações necessárias para o tratamento do pedido. Na sequência, o usuário escolhe a loja na qual deseja realizar o pedido e, antes de finalizar e encaminhar o pedido para a loja, o consumidor escolhe a forma de pagamento, podendo ser *offline* ou *online.* Se a opção for pela primeira forma, o pagamento será por papel moeda ou máquina móvel de cartão; sendo o pedido direcionado diretamente à loja, que utilizará métodos próprios para o pagamento. Quando a forma eleita pelo cliente é

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" (BRASIL, 2018).

[4] De acordo com a LGPD em seu art. 5º, VII: "operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador". (BRASIL, 2018)

[5] A coleta de informações quanto ao modelo de dispositivo utilizado e seu sistema operacional são excessivas e dispensáveis, pois não interferem no pedido do usuário. Trata-se, como se vê, de uma forma invasiva de obter mais informações, o que permitirá o perfilamento daquele consumidor, um dos problemas decorrentes do tratamento de dados pessoais.

online, o pagamento é realizado diretamente ao *marketplace.* Neste caso um terceiro é inserido na cadeia de tratamento de dados pessoais e recebe os dados do cliente, tais como nome completo, data de nascimento, endereço e número do cartão de crédito, débito ou demais dados bancários necessários para a operação. Percebe-se, neste ponto, a inserção de um novo operador de dados pessoais financeiros.

No momento em que o pagamento é aprovado, o pedido é remetido à loja que, ao recebê-lo, tem acesso a dados mais pessoais, tais como: nome, endereço, forma de pagamento, produtos comprados, número de CPF (caso o usuário requeira a nota fiscal identificada) e, em determinados *marketplace's* ainda é coletado o número de telefone do usuário. Na continuidade da prestação dos serviços, alguns desses dados são repassados ao entregador, outro terceiro, responsável por fazer o pedido chegar ao destinatário final. Este último operador entra em contato com dados pessoais tais como nome, telefone e endereço, imprescindíveis para que este finalize o processo, com a entrega ao usuário.

Como se percebe, a operação de compra *on-line*, que parece tão simples e fácil ao consumidor, em realidade coloca em movimento um grande fluxo de dados pessoais compartilhados entre vários agentes de tratamento que atuam na cadeia de fornecimento. Essa dinâmica exige cuidados por parte dos fornecedores, pois além das responsabilidades previstas no Código de Defesa do Consumidor, a partir da LGPD torna-se imperioso observar novos processos para que o tratamento de dados pessoais ocorra em conformidade com a lei e em respeito aos direitos dos titulares, conforme se verá no próximo ponto.

3 TRATAMENTO DE DADOS PESSOAIS NA LGPD: entre oportunidades e riscos ao setor de markeplaces de food delivery

Como visto, o uso das tecnologias promoveu verdadeira reconfiguração dos modos de vida cotidiana, inovando nas formas de relacionar-se, de produzir e consumir produtos e serviços. Tais tarefas, embaladas pelas inovações tecnológicas, permitem a coleta e tratamento de dados pessoais em velocidade e extensão sem precedentes históricos, o que coloca risco à pessoa, sobretudo pelo avanço descontrolado sobre seus dados pessoais.

Com efeito, a avidez do mercado reduz a pessoa à importante fonte de insumo para sua atividade empresarial, a revelar o aprofundamento da fragilidade dos titulares. Essa constatação não é nova e forçou países mais desenvolvidos a editarem, anos antes, normativas mais atualizadas sobre os dados pessoais, com destaque para o Regulamento Geral de Proteção de Dados Pessoais, da União Europeia. Este Regulamento reveste-se de grande importância, não

só por estabelecer um *standard* mínimo aplicável diretamente a todos os países membros do bloco[6], a ser assegurado por uma autoridade reguladora independente e específica (LORENZON, 2021, p.46), mas também por sinalizar ao mercado global a importância que conferiam ao respeito aos dados pessoais, o que seria exigido nas transações comerciais com países terceiros. Essa tomada de posição acabou forçando uma mínima adequação de países terceiros (DONEDA, 2019).

Sob esta inspiração foi editada a Lei Geral de Proteção de Dados brasileira, cujo objetivo central é regulamentar a forma com que as organizações públicas e privadas, com destaque neste trabalho para as empresas que atuam no *marketplaces* de *food delivery*, coletam e tratam dados pessoais em seu poder. Dentre seus fundamentos, destacam-se o respeito à privacidade e o reconhecimento da autodeterminação informativa do titular, tema muito caro aos europeus e que remonta a importantes decisões do Tribunal Constitucional alemão.

Segundo Laura Mendes (2020, p.2), a autodeterminação informativa é um conceito presente em diversos ordenamentos estrangeiros, tendo sido desenvolvido ao longo dos anos a partir de decisões do Tribunal Constitucional da Alemanha, com destaque para a sentença referente ao recenseamento da população. Este direito se constitui em um dos dobramentos do direito ao livre desenvolvimento da personalidade, valorizando a liberdade geral de ação e o respeito à esfera privada dos indivíduos.

A ancoragem no direito geral de personalidade permitiu a abertura do sistema alemão para o reconhecimento de outros direitos (como os dados pessoais) ainda não previstos expressamente em lei naquele momento, o que garantiu maior proteção às pessoas. Trata-se de um importante direito, que se desdobra em três propriedades: 1) poder de decisão do titular; 2) reconhecimento deste direito fundamental como algo flexível, superando a ideia de proteção fixa e determinada e, 3) "a referência pessoal do dado atua decisivamente sobre o teor da proteção na medida em que cada registro que se revela como pessoal é merecedor de proteção". (MENDES, 2020, p. 12). Reforça-se a compreensão de que os conceitos precisam ter uma certa abertura e flexibilidade para acompanhar a evolução tecnológica, sem se prender a classificações rígidas ou fixas de direitos. Partindo dessa e de outras experiências estrangeiras, especialmente o Regulamento Geral de Proteção de Dados da União Europeia, a LGPD elegeu uma série de diretrizes legais e princípios dotados de abertura, os quais devem ser observados

[6] A sua vigência na Europa, a partir de 25 de maio de 2018, inovou no que tange à proteção de dados pessoais em âmbito internacional, por se tratar da primeira regulamentação densa e abrangente sobre o tema, especialmente centrada na pessoa, pois prevê regras e direitos relativos à proteção, tratamento e circulação de dados pessoais (BATISTA; OBREGÓN, 2020, p.10).

por controladores e operadores, em respeito à liberdade e à privacidade dos titulares de dados (PELOSO PIURCOSKY, et al, 2019, p.90).

A LGPD complementa um ecossistema de mais de 40 normas setoriais que regulam de forma direta e indireta a proteção de dados pessoais e a privacidade no Brasil, buscando equilibrar interesses econômicos e sociais. Para tanto, busca limitar eventuais abusos nos processos de tratamento de dados, equilibrando poderes entre indivíduo, o setor privado e o Estado (MONTEIRO, 2018, p. 9) como forma de proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural. Seguindo os passos do Regulamento Europeu, a legislação brasileira se preocupa com o empoderamento dos titulares dos dados pessoais, valorizando a sua autodeterminação informativa, com claro escopo na proteção da pessoa humana e da sua dignidade (IRAMINA, 2020, p. 99).

Além de determinar importantes definições, o art. 6º da legislação elenca princípios orientadores do tratamento, destacando-se a boa-fé, já presente no Código de Defesa do Consumidor, a qual se somam a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, não discriminação e responsabilização. O princípio da boa-fé no tratamento dos dados pessoais desempenha papel relevante, pois possui a função de garantidor o cumprimento da Lei ao impor deveres de conduta aos controladores e operadores, obrigados a agir com probidade e zelo em todas as fases de tratamento de dados, de maneira a assegurar a proteção e segurança adequados (LISBOA, 2019, p. 9) e legitimamente esperados pelo titular. Quando a legítima expectativa do consumidor com relação à segurança jurídica no tratamento de seus dados pessoais não é assegurada, causando-lhe danos, tal situação deve ensejar responsabilidade civil das empresas fornecedoras, como destacam Bioni e Dias (2020).

Os autores se propõem a "construir pontes" entre a legislação consumerista e a LGPD e, para tanto, destacam que a responsabilidade do fornecedor está presente nos dois diplomas legais, constando no art. 14 do CDC e no art. 44 da LGPD. No primeiro caso, a lei é expressa em prever a responsabilidade objetiva em razão de defeitos na prestação de serviços, entendendo como defeituoso quando não fornece segurança ao consumidor, levando-se em consideração circunstâncias como o modo de fornecimento, o resultado e os riscos que dele razoavelmente se esperam, o que deve ser verificado à época em que foi fornecido. A Lei Geral de Proteção de Dados, por sua vez, trata do tema no art. 44 ao dispor sobre a irregularidade no tratamento de dados, assim configurada quando a operação não fornecer a segurança que o titular dele pode esperar, considerando o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam, aproximando sua redação daquela prevista no art. 14, do CDC.

As técnicas de tratamento de dados pessoais disponíveis à época em que foi prestado o serviço também são colocadas como critério de aferição da responsabilidade na LGPD, o que corresponde ao III do art. 14 do CDC, a evidenciar a sintonia entre os diplomas legais (BIONI; DIAS, 2020, s.n.). Apesar da semelhança na redação dos dispositivos, a espécie de responsabilidade se altera radicalmente, pois enquanto o CDC estabelece claramente a responsabilidade objetiva e independente de culpa a LGPD, por sua vez, não foi clara o suficiente, abrindo brechas para que se defenda que a novel legislação contemplou a responsabilidade subjetiva, ancorada na comprovação de culpa do agente de tratamento, no que denunciam como um retrocesso aos direitos do titular.

Com isso percebe-se a importância do princípio da segurança, que impõe que os procedimentos de tratamento devem ser confiáveis para garantir altos níveis de proteção, com adoção de medidas preventivas contra a eventual ocorrência de danos oriundos do tratamento. Essa necessidade determina que o controlador e operador devem se utilizar de dados estritamente necessários para atingir a finalidade do tratamento (REDECKER; BALLICO, 2020, p.139), a evidenciar o entrelaçamento entre a segurança e a finalidade (CRAVO; JOELSONS, 2020). Ao que se vê, esses princípios estão umbilicalmente ligados e são a base para os *marketplaces* de *food delivery* que, como visto, processam inúmeros dados pessoais dos consumidores, incluindo dados para a realização do pagamento.

A LGPD deixa claro que ela impõe uma série de obrigações aos controladores e, dentre elas, pode-se destacar desde procedimentos mais simples e óbvios, como a observância da base legal para o tratamento, até a adoção de outros procedimentos, como notificação ao titular em caso de incidentes de segurança ou violações. Quanto aos riscos, prevê a necessidade de o controlador e o operador elaborarem o relatório de impacto à proteção de dados (RIPD), nos casos indicados (IRAMINA, 2020, p. 99).

Tendo em vista os princípios e obrigações da LGPD, a legislação recomenda que os agentes de tratamento implementem programas de governança em privacidade que, no mínimo, entre outros requisitos, contemplem políticas e salvaguardas adequadas por meio de processo que possibilite avaliações sistemáticas dos impactos e riscos à privacidade, aplicável a todo o conjunto de dados pessoais que o controlador detém (VAINZOF, 2020, p.142).

Um importante programa de privacidade que pode ser implementado é o chamado *privacy by design*, que tem como essência colocar a privacidade em primeiro plano e tratar apenas o mínimo de dados pessoais, necessário para operação do sistema (SCHAAR, 2010, p.271), ou seja, os produtos e serviços devem ser concebidos, desde sua origem, em observância

à proteção de dados pessoais dos titulares[7]. Segundo Souza (2019, p. 427), os elementos que irão permitir o tratamento de dados com proteção da privacidade devem estar incorporados desde o princípio da concepção do produto ou serviço, numa atuação preventiva, ao contrário do que usualmente ocorria, em que era tratado como uma espécie de "adendo" a ser incluído após o incidente de segurança. Portanto, a adoção do *privacy by design* transcende o mero cumprimento dos requisitos previstos na legislação, para avançar sobre os processos desenvolvidos no âmbito da organização, tendo como foco a proatividade e prevenção, com a privacidade já incorporada ao *design*.

Ao tratar do mesmo tema, Carvalho (2019, p. 461) sustenta que além dos princípios que baseiam o conceito de *privacy by design*, as diretrizes estabelecidas pela Norma Técnica ISO/IEC 29100 também devem ser incorporadas, pois descrevem um padrão de garantia da privacidade para os processos produtivos. Prevê que esta será, muito provavelmente, uma tendência no Brasil, especialmente nas grandes companhias, que deverão observá-la como condição para competititidade nos mercados globais. Como se vê, o *privacy by design* é especialmente importante para a atuação dos *marketplaces* de *food delivery*, pois é essencial que todos os partícipes da cadeia de preparação e entrega dos produtos operem de acordo com os padrões legais, aos quais também devem ser agregadas as medidas preventivas, de natureza técnica e administrativa, previstas pelo controlador.

Nesse contexto, mostra-se essencial que os controladores conheçam a legislação e adotem medidas para adequação de suas práticas aos preceitos legais, o que forçosamente irá exigir um plano de conformidade e governança dos riscos. A conformidade também deve ser observada pelos operadores, que no caso do segmento em análise vários atores, incluindo os responsáveis pela entrega, o que aponta para a extensão da responsabilidade, conforme se verá na sequência.

4 A RESPONSABILIDADE DOS AGENTES DE TRATAMENTO: *compliance* e governança como formas de mitigação do risco

A LGPD impôs aos controladores uma série de obrigações que visam à proteção dos

[7] O termo *privacy by desing* significa a implementação de diversos princípios de privacidade diretamente na concepção do produto ou serviço, tornando a privacidade dos dados intrínseca ao sistema, cujo projeto ou concepção já é pensada com essa preocupação de proteger os dados pessoais do titular. Por ser um conceito muito importante, tornou-se uma obrigação legal e um princípio a ser respeitado no Regulamento Geral de Proteção de Dados Pessoais europeu e dali migrou para a legislação brasileira, constituindo-se em instrumental para a mitigação e controle dos riscos do tratamento de dados (ROMANOU, 2018).

direitos fundamentais de liberdade e de privacidade, o que importará na adoção de medidas administrativas e de segurança para proteger os dados pessoais dos usuários. Para tanto, é necessário que os controladores demonstrem que estão legalmente autorizados a realizar o tratamento, ou seja, que o processamento de dados observa uma das bases legais descritas no art. 7º da LGPD. Ademais, precisam evidenciar que possuem recursos de segurança adequados à proteção dos dados e que o tratamento está conforme à finalidade e respeita a privacidade do titular (SILVA, 2020, p.96).

Os artigos 42 e 43 da LGPD elencam as responsabilidades dos controladores e operadores, o que suscita alguns debates entre os estudiosos do tema. Bioni e Dias (2020, p. 5), por exemplo, sustentam que a redação final desses dispositivos se afastou do teor inicialmente previsto na primeira versão do anteprojeto de lei, imperando a responsabilidade subjetiva por força das pressões do mercado. Segundo eles, "Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública em audiência pública realizada na Câmara dos Deputados, essa escolha foi a que prevaleceu no Congresso [...]", e a culpa dos agentes de tratamento precisará ser demonstrada pelo titular dos dados pessoais. Na opinião dos juristas, a escolha por esta espécie de responsabilidade se constituiria em retrocesso, se comparado ao já disposto no CDC.

Ao tratar do tema, Santos, Leitão e Wolkart (2022, p. 70) afirmam que a legislação, ao não ser clara sobre a espécie de responsabilidade adotada, abre margem para vários questionamentos, discutindo se o melhor para a defesa do titular seria recorrer ao Código Civil[8] ou ao CDC. Isso porque o CDC tutela precipuamente o consumidor pessoa natural e destinatário final da prestação, o que limitaria o seu âmbito de incidência, como pontuado no art. 45, da LGPD.

Ademais, como bem lembram Teixeira e Armelin, (2020, p. 308), a responsabilidade civil objetiva do Código Civil pode ser aplicável à LGPD, exigindo-se, para tanto, a análise do risco da atividade, o que coloca em relevo a distinção entre risco inerente e risco adquirido. O primeiro é aquele que está intimamente ligado à própria natureza dos serviços, sendo difícil afastá-lo mesmo recorrendo a técnicas e recursos adequados. O risco adquirido, por sua vez, decorre de cumprimento defeituoso, pois não se trata de atividade que detenha um risco superior ao que legitimamente se espera em condições de normalidade. A atividade torna-se de risco em

[8] Santos, Leitão e Wolkart (2022, p. 69) defendem que, na mesma esteira que a LGPD ampliou o conceito de dados pessoais, adotando uma noção elástica, também evidenciou abertura ao conceituar os agentes de tratamento, que podem tanto ser controlador quanto operadores. A pluralidade de agentes envolvidos aumenta o risco da atividade o que, segundo este entendimento, permitiria utilizar a responsabilidade civil objetiva pelo risco da atividade, prevista no Código Civil.

razão de algum procedimento equivocado ou defeito na prestação.

Aplicando as lições sobre o risco ao setor de *markeplaces de food delivery*, identifica-se que na atividade há um risco inerente, já que o controlador necessariamente atuará junto com outros operadores que, em geral, farão o tratamento de dados, incluindo-se informações sobre a forma de pagamento. Logo, havendo danos decorrentes da violação da segurança dos dados, os agentes de tratamento deverão responder solidariamente, indenizando os eventuais danos, responsabilidade que será excluída em casos expressos no art. 43, da LGPD[9].

Ademais, seus procedimentos não se esgotam em eventual indenização, que sempre chegará tardiamente, pois devem dar ciência aos titulares sobre o tratamento irregular[10] ou eventual incidente, de forma a permitir-lhes a adoção de outros procedimentos para mitigar os prejuízos, tal como o cancelamento de cartões de crédito utilizado, por exemplo. Para tanto, é essencial que os agentes de tratamento tenham um bom sistema de governança de dados pessoais, não somente para prever os riscos, traçar alternativas de prevenção e cuidado em todas os ciclos do seu processamento[11], como também conseguir dar respostas eficientes ao titular dos dados pessoais. Essas boas práticas são incentivadas pelo art. 50 da LGPD, que dispõe sobre a adoção de programas de governança em privacidade, prevendo a estrutura mínima que deve ser adotada (MORAES, 2020, p.51).

Frazão, Oliva e Abílio (2019, p. 681-683), destacam o aspecto preventivo presente na LGPD, especialmente no que se refere às medidas de segurança que devem ser implementadas. Nesse sentido, as organizações precisarão implantar processos de trabalho - desde a concepção do produto até a etapa pós-contratual - que estejam em conformidade com a legislação. Daí resultar tão importante a adoção de boas práticas para orientar todo o fluxo de tratamento de dados dentro da organização. Todas as fases do tratamento devem estar amparadas na

[9] O artigo 43 elenca as hipóteses que afastam a responsabilidade, sendo apenas três: o agente comprovar que não realizou o tratamento; a segunda excludente depende de comprovação de que mesmo realizando o tratamento, não houve violação à LGPD e a última hipótese exige que seja comprovado que o dano causado é de culpa exclusiva do titular (CAPANEMA, 2020, p. 166). Percebe-se que em regra, havendo problema ou incidente de segurança que coloque em situação de risco ou vulnerabilidade os direitos do titular haverá responsabilização por parte do controlador, o que pode ser ampliado para responsabilidade solidária, caso o operador também tenha atuado no tratamento.

[10] O art. 44 refere as situações em que o tratamento de dados pessoais pode ser considerado irregular, não se limitando apenas ao que está na LGPD, pois seu rol de irregularidades é exemplificativo (OLIVEIRA; PORTO, 2020, p.113). Para aferir sua irregularidade deve-se levar em conta elementos como: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

[11] O que por certo abarca a fase de armazenamento e conservação dos dados, pois o art. 47 da LGPD determina que os agentes de tratamento (o que inclui o controlador) ou qualquer outra pessoa que intervenha em uma das fases do tratamento deva garantir a segurança da informação em relação aos dados pessoais, inclusive após o término do tratamento (JIMENE, 2020, p. 33).

legislação, o que evidencia a importância dos programas de *compliance*, ou seja, ações articuladas no ambiente organizacional, abarcando todos os atores implicados, que devem agir preventivamente para evitar a ocorrência de incidentes de segurança ou, ainda, mitigar os eventuais danos deles decorrentes (FRAZÃO, OLIVA, ABÍLIO, 2019, p. 681-683).

Tais programas devem estabelecer os controles internos que vão permitir que os agentes de tratamento estejam de acordo com a lei. Regulação e *compliance* passam a ser vistos como complementares, pois há uma influência entre a regulação estatal e o modelo a ser adotado pelas organizações, que devem estabelecer seus processos internos levando em conta as características de sua atuação. Trata-se de uma complementaridade entre a previsão emanada do Estado, via legislação, e as normas e padrões de conduta, de iniciativa privada, que devem ser observados por todos os membros da organização (FRAZÃO, OLIVA, ABÍLIO, 2019, p. 684).

A demonstração de que a organização está *compliance* no tratamento dos dados pessoais será importante elemento, pois tanto auxiliará na prevenção de incidentes de segurança, quanto, caso ocorram, demonstrarão que o controlador agiu de boa-fé ao tratar dos dados pessoais de seus clientes e colaboradores.

Resta evidente que a LGPD determina aos controladores a implementar medidas de segurança, técnicas e administrativas, que tenham a capacidade de efetivamente proteger os dados pessoais de acessos não autorizados e contra incidentes que coloquem em risco a privacidade dos titulares (BOTELHO, 2020, p. 221). Essas medidas se evidenciam em políticas corporativas de proteção de dados pessoais, contratos de confidencialidade, políticas de privacidade de sites e aplicativos, capacitação dos empregados e colaboradores que realizam tratamento de dados, controle do acesso aos arquivos físicos e digitais, alinhamento da atividade entre controlador e operadores, entre outras adequações que devem ser promovidas. Ademais, com a vigência da LGPD há a necessidade de revisão, por parte dos controladores, dos modelos de governança de segurança da informação já existentes adicionando-se, quando necessário, o relatório de impacto à proteção de dados pessoais (RIPD) e a matriz de risco de dados pessoais, novos instrumentos para mensurar o risco e propor procedimentos de mitigação e salvaguarda. Trata-se de inovação adotada pela LGPD, pois não havia, anteriormente, legislação que obrigasse os controladores a protegerem dados pessoais com esse grau de exigibilidade (JIMENE, 2020, p. 46; SILVA, 2020, p.97).

Veja-se que não é suficiente que o controlador esteja em *compliance* com a LGPD, pois se ele transfere dados para operadores, como ocorre no caso do segmento analisado, também poderá responder solidariamente por eventual falha gerada pelo operador. Há, portanto, um

acréscimo de responsabilidade, pois caberá ao controlador também buscar parceiros de negócios que igualmente observem a lei, sob pena de ter problemas decorrentes dos incidentes de segurança.

O maior objetivo da governança corporativa é assegurar que os dirigentes das organizações atuem no interesse conjunto dos acionistas, terceiros vinculados à atividade empresarial como titulares de dados (receptores de serviços, consumidores) e não apenas no próprio interesse da corporação. Portanto, a atuação em conformidade com a LGPD deve incorporar diversas variáveis, tais como: transparência na divulgação de informações; implementação de sistemas de controle interno; gerenciamento dos riscos e conformidade da operação com a leis, sendo que o conceito de *compliance* tem relação direta com programas que assegurem as boas práticas de governança corporativa (PINTO JUNIOR, 2017, p.52). Quando efetivamente funciona, o *compliance* tem como função assegurar que inconformidades sejam evitadas ou minimizadas, consistindo em importante mecanismo de proteção e aprimoramento de reputação corporativa, pois garante que os principais processos organizacionais sejam realizados em conformidade com a legislação vigente (AZEVEDO; *et al*, 2017, p. 182).

A LGPD em seu artigo 5°, XVII prevê uma importante ferramenta de governança, o relatório de impacto à proteção de dados pessoais (RIPD)[12], que dá efetividade a diversos princípios da LGPD. Este dispositivo contempla a adoção de medidas técnicas e administrativas aptas a proteger dados pessoais, a adoção de medidas de prevenção a ocorrência de danos em razão do tratamento dos dados e a demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento da LGPD, demonstrando a eficácia das medidas adotadas (VAINZOF, 2020, p.141). O RIPD é uma importante ferramenta de governança, intrínseco às atividades de tratamento que permite medidas que garantem a conformidade com a lei, bem como permitem demonstrar uma atitude *privacy by design* do controlador (VAINZOF, 2020, p.155).

Compreende-se que a gestão de riscos é inerente a qualquer atividade e parte fundamental para o desenvolvimento das organizações, podendo ser utilizada de forma a potencializar resultados, explorar e identificar oportunidades ou, ainda, mitigar perdas e prejuízos. Sua importância é vital para balizar a atuação do controlador à luz da atividade que

[12] O Art. 5º, inciso XVII assim dispõe: "relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco [...]"

realiza, pois há distintas espécies de graus de risco. Segundo Azevedo et al. (2017, p. 186), os riscos podem ser caracterizados como: a) especulativos, que correspondem a uma possibilidade de ganho ou perda; b) puros, nos quais há uma chance de perda sem possibilidades de ganhos. De acordo com a origem, podem ser divididos em ricos internos, que se originam dentro da organização ou externos a sua operação, quando advém de terceiros (AZEVEDO et al, 2017, p. 186).

A implementação de ferramentas de governança pressupõe a identificação e classificação dos riscos, atividade para a qual é importante a colaboração de todos os atores envolvidos, incluindo o comprometimento e engajamento dos integrantes da administração. O processo precisa ser *top down*, ou seja, de cima para baixo, iniciando-se na alta administração e se espalhando aos demais setores de forma organizada e controlada (AZEVEDO et al, 2017, p.188). Desta forma a construção do RIPD deve ser realizada em conjunto com a alta administração, principalmente para uma organização que realiza o tratamento de dados como atividade principal, tendo em vista que os resultados do relatório podem impactar toda a operação. Ademais, é preciso compreender que se trata de uma avaliação de impactos que objetiva mapear, planejar, implementar e monitorar o processo de tratamento dentro da conformidade legal e, nessa perspectiva, precisa acompanhar a dinâmica da organização e ser constantemente atualizado para garantir a preservação dos direitos dos titulares dos dados (GOMES, 2019, p. 211).

Trata-se de documentação que o controlador deve utilizar para descrever os processos de tratamento de dados pessoais a fim de identificar riscos durante o tratamento e elencar medidas de segurança e salvaguardas (GOMES, 2019, p.212). Possui uma diretriz sistemática das operações de tratamento de dados para viabilizar a visualização e gestão dos processos e procedimentos internos de tratamento de dados pessoais, para que a partir dele seja possível criar mecanismos de prevenção e mitigação dos riscos (GOMES, 2019, p. 211).

5 CONCLUSÃO

O mercado de *food delivery* está em constante expansão devido às facilidades que proporciona aos seus usuários, o que foi acelerado pela pandemia da COVID-19. A tecnologia no setor é o centro de toda operação entre aplicativos, restaurantes e clientes, sendo imprescindível que os *marketplaces* realizem ações para se adequarem às normativas de proteção de dados pessoais vigentes.

A LGPD é clara em estipular princípios e parâmetros para o tratamento de dados

pessoais e, dessa forma, os *marktplaces* devem considerar todos os envolvidos no tratamento. Essa visão sistêmica é importante, especialmente porque neste segmento o tratamento de dados ocorre desde os restaurantes, passando pelos entregadores e outros eventuais partícipes. Em alguns momentos do ciclo do pedido, tais terceiros possuem acesso a diferentes dados, cujo conhecimento é importante para que cada um cumpra com a sua função, possibilitando que o produto seja entregue ao consumidor. Esse processo que envolve múltiplos atores evidencia a necessidade da adoção de ferramentas administrativas que objetivam à segurança desses dados, tendo em vista que a normativa brasileira considera como responsável pelo dano tanto o operador quanto o controlador, havendo a hipótese de responsabilidade solidária.

As práticas de governança e *compliance* possuem por objetivo controle e mitigação dos riscos das operações de tratamento de dados pessoais e a própria LGPD, em seu art. 38, as considera como importante estratégia. Segundo este dispositivo, a Autoridade Nacional de Proteção de Dados pode determinar ao controlador a elaboração do RIPD, pois ele fornece informações sobre como ocorre o tratamento dos dados, níveis de risco atribuídos ao tratamento e possibilita a identificação, em processos internos, de eventuais falhas de tratamento.

O segmento do *marketplaces* de *food delivery* tem grandes desafios, pois vários atores interferem em diferentes etapas do processo (operadoras de pagamento online, restaurantes e entregadores) e realizam o tratamento de dados pessoais. As especificidades do trabalho de cada agente podem impor o acesso a outros dados, tais como CPF do usuário, o que exige um fluxo de tratamento claro, de acordo com as finalidades para o qual aquele dado pessoal foi recolhido, em respeito à legislação. A efetividade da proteção prevista em lei exige que os *marketplaces* adotem processos de governança e *compliance* que envolvam todos os partícipes que operam no sistema, que igualmente precisam compreender o alcance da LGPD e suas exigências, especialmente porque realizam o tratamento dos dados coletados pelos *marketplaces*.

Portanto, defende-se que o sistema utilizado por todos os agentes deva pautar-se em políticas de *compliance* e governança orientadas por boas práticas, o que deve envolver desde a concepção do processo e todas as fases de execução, incluindo a pós-entrega. Todas as etapas devem ser concebidas e executadas em conformidade com o conceito *privacy by design*, ou seja, tratar o mínimo necessário de dados durante sua operação. Tal conceito, alinhado com o RIPD, possui fortes implicações na gestão do risco durante o tratamento de dados realizado, principalmente considerando a quantidade de agentes envolvidos que, por serem empresas de menor porte, podem ter mais dificuldade em se adequar aos requisitos previstos na LGPD. Portanto, para o cumprimento da LGPD e sua implementação, o *marketplace* deve tomar para

si a responsabilidade de se adequar e orientar seus parceiros de negócios para atuação responsável e em respeito aos direitos dos titulares de dados, aplicando políticas de governança e *compliance* como importantes ferramentas para controle, gestão e mitigação do risco oriundo do tratamento de dados. Não obstante toda essa gestão, se mesmo assim o incidente de segurança ocorrer e gerar danos, tais devem ser indenizados, aplicando-se a responsabilidade objetiva, quer porque se trate de relação de consumo, a ensejar o diálogo entre o CDC e a LGPD; quer baseada na gestão do risco, para o que poderá buscar apoio no art. 927, parágrafo único, do Código Civil.

REFERÊNCIAS

AKHMADI, Heri; PRATOLO, Suryo. Online Marketing of Food Products through Marketplace Platform: A Study of Community Based Online Marketplace of BEDUKMUTU. In: **E3S Web of Conferences 232**, *02015 (2021)*. Disponível vem: https://www.e3s-conferences.org/articles/e3sconf/pdf/2021/08/e3sconf_iconard2020_02015.pdf. Acesso em: 26 mar. 2023.

AZEVEDO, Mateus Miranda de et al. O compliance e a gestão de riscos nos processos organizacionais. **Revista de Pós-graduação Multidisciplinar**, [S.l.], v. 1, n. 1, p. 179-196, june 2017. ISSN 2594-4797. Disponível em: <http://www.fics.edu.br/index.php/rpgm/article/view/507>. Acesso em: 09 nov. 2021.

BATISTA, Luana Scandian; OBREGÓN, Marcelo Fernando Quiroga. Os impactos do regulamento europeu geral sobre proteção de dados (EU GDPR) no Brasil. **Derecho y Cambio Social.** n.62. outubro – dezembro. 2020. Disponível em: https://www.derechoycambiosocial.com/revista062/sumario62.html Acesso em: 23 out. 2021.

BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor**. Civilistica.com**, v. 9, n. 3, p. 1-23, 22 dez. 2020.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas–Unifafibe**, v. 8, n. 2, 2020. Disponível em http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf Acesso em: 5 de nov. 2021.

BRASIL. **Lei nº 13.709, 2018. Lei Geral de Proteção de Dados (LGPD)**. 2018, Brasília, DF. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 27 mai. 2021.

CAPANEMA, Walter Aranha. A responsabilidade civil na lei geral de proteção de dados. **Cadernos Jurídicos**, São Paulo, ano 21, n°53, p. 163-170. Janeiro/Março, 2020. Disponível em https://core.ac.uk/reader/322682320 Acesso em: 05 nov. 2021.

CARVALHO, Angelo Gamba Prata de. Transferência internacional de dados na Lei Geral de Proteção de Dados - Força normativa e efetividade diante do cenário transnacional. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 621-645.

CRAVO, Daniela Copetti; JOELSONS, Marcela. A importância do CDC no tratamento de dados pessoais de consumidores no contexto de pandemia e de vacatio legis da LGPD. **Revista de Direito do Consumidor**, 2020. Disponível em https://www.researchgate.net/profile/Marcela-Joelsons-2/publication/352131773_A_IMPORTANCIA_DO_CDC_NO_TRATAMENTO_DE_DADOS_PESSOAIS_DE_CONSUMIDORES_NO_CONTEXTO_DE_PANDEMIA_E_DE_VACATIO_LEGIS_DA_LGPD/links/60ba40cd299bf10dff96e2d3/A-IMPORTANCIA-DO-CDC-NO-TRATAMENTO-DE-DADOS-PESSOAIS-DE-CONSUMIDORES-NO-CONTEXTO-DE-PANDEMIA-E-DE-VACATIO-LEGIS-DA-LGPD.pdf Acesso em: 12 nov. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, p. 677-715.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. **Revista do Advogado**, São Paulo, n. 144, p. 6-15, 2019. Disponível em http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Dir-Soc-Pol-Publicas_v.8_n.2.08.pdf Acesso em: 7 nov. 2021

IRAMINA, A. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, 2020.

JIMENE, Camilla do Vale. Da importância da segurança da informação para adequação à LGPD. In: OPICE BLUM, Renato. **Proteção de dados**: Desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020, p. 39-48.

LISBOA, Roberto Senise. Boa-fé e confiança na LGPD brasileira. **Revista do Advogado da AASP,** 2019. Disponível em https://www.academia.edu/42604203/Boa_f%C3%A9_e_confian%C3%A7a_na_LGPD_brasileira Acesso em: 02 nov. 2021.

LORENZON, Lalla Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de *enforcement*. In: ALMEIDA, Paulo Wojcikiewicz, **Revista do Centro de Excelência Jean Monnet da FGV Direito Rio.** V. 1. Rio de Janeiro: FGV Direito Rio, 2021.

LUCA, Michael. Designing online marketplaces: trust and reputation mechanisms. **Innovation Policy and the economy.** v. 17, p. 77-93, 2017. Disponível em https://www.journals.uchicago.edu/doi/full/10.1086/688845 Acessso em: 14 mai. 2021.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar-Revista de Ciências Jurídicas**, v. 25, n. 4, 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 26 mar. 2023.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil. **Artigo estratégico**, v. 39, p. 1-14, 2018. Disponível em https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf Acessado em 02 de Junho de 2021.

MORAES, Henrique Fabretti. Data protection officer – papéis, responsabilidades e boas práticas. In: OPICE BLUM, Renato. **Proteção de dados**: Desafios e soluções na adequação à lei. Rio de Janeiro: Forence, p.49-62, 2020.

OLIVEIRA, Priscila Gois de; PORTO, Antonio Augusto Cruz. Direito à privacidade dos indivíduos na lei geral de proteção de dados n° 13.709/2018 – LGPD. **Revista de Direito UTP**, v.1, n.1, p, 99-117, jul/dez, 2020. Disponível em https://interin.utp.br/index.php/DRT/article/view/2503/2084 Acesso em: 02 nov. 2021.

PELOSO PIURCOSKY, Fabrício et al. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma Neg**., Bogotá, v. 10, n. 23, p. 89-99, Dec. 2019. Disponível em http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S2215-910X2019000300089&lng=en&nrm=iso&tlng=pt Acesso em: 04 jun. 2021.

PINTO JUNIOR, Mario Engler. Corrupção, governança, ética e compliance. **Revista de Direito da Empresa e dos Negócios,** v. 1, n. 1, p. 41-56, 2017. Disponível em <http://revistas.unisinos.br/index.php/rden/article/view/14292/6019> Acesso em: 03 nov. 2021.

REDECKER, Ana Cláudia; BALLICO, Louise Finger. O papel dos agentes na lei geral de proteção de dados (LGPD). **Revista Jurídica Luso-Brasileira**. n. 5, p. 125-170, 2020. Disponível em https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-6-2020-n-5/211 Acesso em: 24 out. 2021.

ROMANOU, Anna. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise, **Computer Law & Security Review**, Volume 34, Issue 1, p. 99-110, 2018. Disponível em <https://www.sciencedirect.com/science/article/pii/S0267364917302054> Acesso em: 10 nov. 2021.

SANTOS, Rômulo Marcel Souto dos; LEITÃO, André Studart; WOLKART, Erik Navarro. A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A REGRA DE HAND. **Revista Opinião Jurídica** *(Fortaleza),* Fortaleza, v. 20, n. 34, p. 60-84, mar. 2022. ISSN 2447-6641. Disponível em: https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/4179. Acesso em: 03 abr. 2023. doi:http://dx.doi.org/10.12662/2447-6641oj.v20i34.p60-84.2022.

SCHAAR, Peter. Privacy by design. **Identity in the Information Society**, v. 3, n. 2, p. 267-274, 2010. Disponível em https://link.springer.com/content/pdf/10.1007/s12394-010-0055-x.pdf Acesso em: 23 nov. 2021.

SEE-KWONG, G., SOO-RYUE, N., SHIUN-YI, W., & LILY, C. Outsourcing to Online Food Delivery Services: Perspective of F&B Business Owners. **The Journal of Internet Banking and Commerce**, 22, p. 1-18, 2017. Disponível em https://www.icommercecentral.com/open-access/outsourcing-to-online-food-delivery-services-perspective-of-fb-business-owners.php?aid=86136 Acesso em: 15 jun. 2021.

SILVA, Laércio de Souza. Soluções de tecnologia para a gestão da governança em privacidade e a implementação da LGPD. In: OPICE BLUM, Renato. **Proteção de dados***:* Desafios e soluções na adequação à lei. Rio de Janeiro: Forence, p.95-109, 2020.

SOPRANO, Paula. Faturamento do ecommerce cresce 122% e empresas investem em infraestrutura. **Folha de São Paulo**, 28 de dezembro de 2020. Disponível em www1.folha.uol.com.br/mercado/2020/12/faturamento-do-ecommerce-cresce-122-e-empresas-investem-em-infraestrutura.shtml Acesso em: 10 abr. 2021.

SOUZA, Carlos Affonso Pereira de. Segurança e sigilo dos dados pessoais: primeiras impressões à Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 417-441.**

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. A responsabilidade e ressarcimento de danos por violação às regras previstas na LGPD: Um cotejamento com o CDC. In: LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020, p. 297-326.

VAINZOF, Rony. Relatório de impacto à proteção de dados pessoais. In: OPICE BLUM, Renato. **Proteção de dados:** Desafios e soluções na adequação à lei. Rio de Janeiro: Forence, p.141-167, 2020.

ÇAVUŞOĞLU, M. (2012). Electronic Commerce And Turkish Patterns of Online Food Delivery System. **Journal of Internet Applications and Management**, 3 (1), 45-62. DOI: 10.5505/iuyd.2012.44153. Disponível em dergipark.org.tr/en/pub/iuyd/article/377309#article_cite Acesso em 10 jun. 2021.