DIREITO & TI
FABIN ISSN 2447-1097
WWW.DIREITOETI.COM.BR

Contratos digitais: a manifestação do consentimento sob a perspectiva da Lei Geral de Proteção de Dados

Digital Contracts: consent manifestations under the General Data Protection Law perspective

Heitor Leite França[1]
Luiz Felipe da Fonseca Pereira[2]

Recebido em: 07.10.2024
Aprovado em: 29.09.2025

RESUMO

A presente pesquisa objetiva discutir o exercício da autodeterminação informativa do titular dos dados nos contratos digitais através da manifestação do consentimento. Fez-se necessária uma reflexão crítica no que tange aos contratos digitais e a forma de como se encontram estruturados, dado que o problema de pesquisa reside no questionamento sobre a forma pela qual o protagonismo oferecido pela LGPD aos titulares dos dados é consolidado nos contratos digitais, o que levou à conclusão de que o modo de exaração do consentimento do titular diante dos entes de tratamento de dados é precário, razão pela qual levantou-se possíveis frentes de solução legal pertinentes à querela em epígrafe. Para os fins de elaboração do estudo em epígrafe, foi utilizado o método dedutivo de pesquisa, com a adoção da abordagem qualitativa em conjunto com a técnica bibliográfica e documental.

Palavras-chave: Autodeterminação informativa; Consentimento; Contratos digitais; Desvirtuamento; Lei Geral de Proteção de Dados.

ABSTRACT

This research aims to discuss the exercise of informational self-determination by data subjects in digital contracts through the expression of consent. A critical reflection on digital contracts and their structural design was necessary, given that the research problem lies in questioning how the protagonism granted by the brazilian general data protection Law (LGPD) to data subjects is effectively consolidated in digital contracts. This led to the conclusion that the way in which the data subject provides consent to data processing entities is precarious, which prompted the study and identification of possible legal

[1] Pós-graduando em direito e processo tributário no Centro Universitário FIBRA. E-mail: heitorfranca121@gmail.com. Lattes: http://lattes.cnpq.br/1670569807499498.
[2] Advogado. Doutorando em Direito pela Universidade Federal do Pará – UPFA. Consultor do Projeto Elos do MCTI. Assessor Jurídico da Agência Reguladora de Belém - ARBEL. Professor de Direito Público. Vice-líder do Grupo de Pesquisa Financiando Direitos. Lattes: http://lattes.cnpq.br/6354404605022151.

avenues to address the issue at hand. For the purposes of this study, the deductive research method was employed, adopting a qualitative approach combined with bibliographic and documentary research techniques.

Keywords: General Data Protection Law; Digital contracts; Informational self-determination; Consent; Distortion.

1 INTRODUÇÃO

Com o advento das Tecnologias da Informação e Comunicação - TIC´s, o mundo se inseriu em um contexto no qual a informação passou a ser vista como um recurso mercadológico, notadamente pelo seu potencial de geração de riqueza àqueles que a possuem.

A economia dos dados inserida na sociedade da informação consiste essencialmente na compra e venda de dados coletados pelas grandes corporações de TIC para fins de divulgação de publicidade direcionada aos consumidores, publicidade essa promovida por anunciantes, os quais lucram com as vendas que efetuam com maior segmentação ao seu público alvo, em detrimento da privacidade.

A ambição lucrativa das grandes corporações de TIC ensejou grande preocupação das autoridades governamentais sobre o modo de como os dados estavam sendo tratados, principalmente no que tange aos métodos de obtenção dos referidos recursos.

A necessidade de proporcionar um maior domínio dos titulares dos dados no tratamento de suas informações pessoais moveu, no âmbito internacional, notadamente por parte da União Europeia, a produção de mecanismos jurídicos reguladores de relações entre titulares e entes de tratamento de dados, tendo sua concretização com o advento da *Data Protection Directive*, ou seja, Diretiva de proteção de dados 95/46/EC.

Cerca de 21 anos mais tarde, a Diretiva deu lugar ao *General Data Protection Regulation* - Regulamento Geral de Proteção de Dados – GDPR, assinado em 2016 e vigorado em meados de 2018, com o objetivo de adequar a regulação governamental à exponencial evolução da tecnologia.

O advento do GDPR se deu pela necessidade de uma nova legislação capaz de abranger um acervo de concepções e frentes de tutela jurídicas mais ajustadas às

dinâmicas sociais contemporâneas, além de consolidar prescrições normativas aplicáveis a todos os Estados-membros do bloco europeu, o que não fora observado pela Diretiva 95/46/EC, a qual se limitava a delegar competências, a fim de que cada um dos estados-membros do bloco europeu legislasse conforme a sua realidade fático-jurídica (Ferreira, 2018).

Em se tratando do âmbito nacional, a discussão sobre a necessidade de se instituir uma lei capaz de tutelar a proteção dos dados pessoais teve um início tardio. O PL 4060/2012 de autoria do deputado Milton Monti incorporava, em sua justificativa, a mesma preocupação tida pelos países europeus frente aos crescentes dinamismos da tecnologia da informação (Brasil, 2012).

O aludido projeto que, mais tarde, veio a despontar na Lei ordinária 13.709/2018 (Lei Geral de Proteção de Dados), revelou uma verdadeira importação de parâmetros já adotados na comunidade internacional, tendo, como um de seus fundamentos, a autodeterminação informativa (FIA, 2019).

As legislações europeia e brasileira, ressalvados alguns pontos de divergência entre perspectivas[3], foram convergentes, dentre outros núcleos de tutela legal, em posicionar o consentimento do titular dos dados como um dos pontos principais de suas respectivas disciplinas jurídicas, dada a situação de hipossuficiência e vulnerabilidade deste em comparação às empresas de TIC (Gomes; Bittencourt, 2019).

O presente trabalho buscará identificar como a autodeterminação informativa é concretizada nos termos e condições de uso das empresas de TIC, tendo-se como referência a Meta (Facebook), na sua condição de empresa pioneira no ramo, dado o seu acervo de aplicações integradas a serviços de direcionamento de publicidade, baseada no

[3] O art. 5° da LGPD (Brasil, 2018), ao dispor que o consentimento é "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", demonstra um viés subjetivista ao titular dos dados, no sentido de concentrar a tutela legal no ato volitivo do titular dos dados em anuir com termos e condições de uso de serviços de agentes de tratamento, sem, contudo, dispor de maneira clara quanto ao processo de obtenção do seu consentimento a ser seguido pelas referidas entidades. De modo diverso, o GDPR (UE, 2016) demonstra um caráter objetivista nas relações digitais, notadamente pela disposição de seus artigos legais, os quais exigem proatividade por parte de agentes de tratamento, visando prover a informação e proteção do titular dos dados, mediante o estabelecimento de critérios legais objetivos.

rastreamento e coleta de dados de seus usuários, com vistas a aferir, no plano da eficácia legal, as disposições da LGPD no que tange à legitimação do consentimento do titular dos dados, sem prejuízo de analogias com o Regulamento Geral de Proteção de Dados europeu.

O artigo abordará, de maneira informativa e investigativa, se o advento da LGPD teve efeitos concretos no que tange à garantia do protagonismo do titular dos dados, no contexto do modo de como o seu consentimento é obtido. Para tais fins, foi utilizado o método dedutivo, de modo a expandir, a outros modelos de contratos digitais, as conclusões alcançadas no presente estudo. Como técnica de pesquisa, adotou-se a análise bibliográfica de artigos acadêmicos, leis vigentes, doutrinas e matérias de sites especializados.

O estudo, assim dividido em cinco momentos, é inaugurado a partir da apresentação de duas definições interdependentes entre si: o consentimento e a autodeterminação informativa, acepções essas que ensejarão toda a investigação do artigo científico.

Em uma segunda abordagem, tratar-se-á a respeito dos desafios da concretização do consentimento do titular dos dados nos moldes da LGPD com vistas ao panorama atual dos contratos digitais, bem como alusões ao uso de tecnologias evasivas ao controle legal por parte de agentes de tratamento de dados, dentro da economia digital.

Em sua terceira parte, a pesquisa se concentra na análise dos contratos digitais feitos junto a empresa Meta de modo a explorar como as políticas de uso são efetivadas na perspectiva do titular dos dados, contextualizada aos ditames da Lei Geral de Proteção de dados com vistas a aferir a conformidade de tais modelos de negócio com os direitos garantidos pela referida lei frente ao seu propósito de oferecer um maior controle dos titulares de dados pessoais quanto ao fluxo de suas informações oferecidas aos entes de tratamento de dados.

À quarta etapa do presente estudo, buscar-se-á, com fulcro nas análises realizadas no decorrer da pesquisa, promover reflexões panorâmicas fulcradas em resultados alcançados, de modo a estendê-los ao contexto atual dos contratos digitais, inseridos no âmbito da concretização do consentimento e autodeterminação informativa.

Na quinta e última frente de discussão do artigo, far-se-á um arrazoado conclusivo sobre a pesquisa, de modo a repisar discussões estabelecidas, no sentido de promover a conscientização do leitor e apresentar possíveis soluções concretas, contextualizadas na esfera legislativa, à problemática da pesquisa.

2 CONSENTIMENTO DO TITULAR: DESAFIOS AO PROTECIONISMO DA LGPD

Desde o seu advento, a Lei Geral de Proteção de Dados conferiu ao jurisdicionado um maior controle sobre as informações que fornece aos entes de tratamento de dados.

Contudo, é mister a abordagem introdutória pertinente à resistência por parte da realidade fática em se permitir o exercício das prerrogativas legais dos titulares dos dados, ocasião na qual se ilustrará as evasões por parte de entes de tratamento em consultar a anuência do titular dos dados.

2.1 Consentimento e a autodeterminação informativa: definições e interdependência de institutos

Em termos apriorísticos, é de substancial importância compreender os institutos "consentimento" e "autodeterminação informativa" em suas respectivas acepções legais, visto aquele primeiro se afigurar como um instrumento de concretização deste último.

O consentimento é um instituto cuja conceituação legal é prevista especificamente no art. 5°, XII da Lei Geral de Proteção de Dados, o qual o define como toda "manifestação **livre**, **informada** e **inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma **finalidade determinada**" (Brasil, 2018, grifos do autor).

Do compulso da leitura do referido diploma legal, é nítida a presença de quatro pilares de existência do consentimento: liberdade, informação, certeza e finalidade específica.

Destaque-se, dentre eles, o pilar da liberdade, para fins de melhor compreensão do conceito da autodeterminação informativa que, inobstante prevista como um dos fundamentos da lei de proteção de dados pessoais, mais especificamente na redação de seu art. 2°, II, se apresenta eivado de obscuridade, se interpretado de modo superficial.

Por esta razão, Vainzof (2019, p. 24, grifos nossos) em didática e contextualizada explicação se propôs a definir tal instituto:

> [...] a quantidade de dados disponíveis e a qualidade de seu tratamento por meio de sistemas informatizados altamente capazes [de processá-los] transformaram dados pessoais em verdadeiras commodities. Modelos de negócios são invariavelmente pautados e rentabilizados, cada vez mais, no tratamento de dados pessoais.
> De tal sorte, pensar que o cidadão possa ter o controle sobre seus próprios dados parece, atualmente, utopia. Porém, a autodeterminação informativa se apresenta como fundamento da LGPD, justamente nesse momento em que ainda predomina uma coleta e tratamento massivo e desenfreado de dados, como forma de devolver para o titular o poder sobre o fluxo e o uso dos seus próprios dados, mediante o estabelecimento de determinações objetivas aos agentes de tratamento.
> **A autodeterminação informativa, que é o controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático [em que bastaria garantir o direito de recusa ou proibição do titular como exclusão do conhecimento de terceiros]; e a moderna, em que a intervenção (proteção) [dos dados] é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular.** Nas palavras de Stefano Rodotà é um "poder permanente de controle sobre seus próprios dados".

É essencial a interpretação sistemática dos dois institutos, agora devidamente conceituados, no que tange ao estudo das relações entre os titulares dos dados e os agentes de tratamento.

Considerando-se que, no que diz respeito ao ambiente virtual, meio pelo qual incontáveis relações contratuais são firmadas entre os seus respectivos pactuantes, o consentimento do titular, além de ser uma nítida manifestação volitiva em contratar, é, também, uma concretização da *liberdade* em contratar.

Tomando-se por base os fundamentos alhures mencionados, fica, assim, demonstrada a relação de interdependência entre ambos os institutos em epígrafe, visto

que, sem consentimento não há autodeterminação e, sem esta última, não há aquele primeiro.

Dada a importância dos institutos, a LGPD e a sua paragonada legislação europeia, *General Data Protection Regulation* – GDPR, demonstram um protecionismo concorrente no que tange à garantia do protagonismo dos titulares dos dados. Conforme aduzem Gomes e Bittencourt (2019, p. 29):

> O consentimento é um tema chave tanto na legislação europeia, quanto na brasileira e sem ele o responsável pelo tratamento dos dados não pode fazer nada. Ambas normativas trazem o indivíduo como ocupante do lugar central na proteção dos dados pessoais.

Note-se que a aferição do consentimento no ambiente virtualizado requer cautelas específicas para fins de legitimação da vontade em contratar do titular dos dados em decorrência da sua vulnerabilidade técnica diante dos entes de tratamento.

Assim, abordar-se-á a realidade fática das relações entre titulares e agentes de tratamento de dados, de modo a demonstrar que, inobstante os esforços legais para a regulação das referidas interações entre ambos os polos retromencionados, o saneamento e controle de abusos ainda permanece como um desafio concreto.

2.2 O desvirtuamento do consentimento do titular dos dados em contratos digitais

Em se tratando das relações contratuais entre titulares e entes de tratamento de dados no meio eletrônico, os contratos de adesão correspondem à regra geral. Mister lembrar que tal espécie de negócio jurídico tem como sua essência principal a indiscutibilidade das cláusulas contratuais, cabendo ao contratante, ora aderente, tão somente a prerrogativa de anuir ou não com os termos que lhe são apresentados. Ainda neste ínterim, leciona Gonçalves (2019, p.122) que:

> Contratos de adesão são os que não permitem essa liberdade [de discutir livremente as suas cláusulas e condições], devido à preponderância da vontade de um dos contratantes, que elabora todas as cláusulas. O outro adere ao modelo de contrato previamente confeccionado, não podendo modificá-las:

> aceita-as ou rejeita-as, de forma pura e simples, e em bloco, afastada qualquer alternativa de discussão.
> [...]
> No contrato de adesão deparamos com uma restrição mais extensa ao tradicional princípio da autonomia da vontade. [...] O indivíduo que necessita contratar com uma grande empresa exploradora de um serviço público depara com um contrato-padrão, previamente elaborado, limitando-se a dar a sua adesão ao paradigma contratual já estabelecido. Ou se submete a ele, sem chance de discutir o preço e outras condições propostas, contratando, ou se priva de um serviço muitas vezes indispensável.

A querela não se concentra na adoção da modalidade contratual em epígrafe entre os contratantes, mas sim no modo de como os contratos se encontram estruturados, os quais - justamente por não comportarem ajustes bilaterais entre aqueles que os firmam - dificultam a detecção de ilegitimidades e/ou disposições abusivas, viciando, assim, a exaração do consentimento do titular dos dados que, movido pela indispensabilidade de determinada aplicação digital, consinta sem, contudo, ter ciência do destino, tampouco do modo de processamento das informações pessoais que fornece ao entes de tratamento.

Deste modo, o consentimento, o qual deveria se configurar como manifestação legítima do exercício da autodeterminação informativa, se rebaixa a um mero ratificador de contratos digitais, resultando assim no fenecimento de sua função como instrumento de controle de ilegitimidades contratuais, que poderia ser exercido pelo próprio titular dos dados pessoais, dentro de suas prerrogativas que lhe foram legalmente concedidas pela LGPD. A respeito, consignam Gomes e Bittencourt (2019, p. 30) que:

> [...] é curioso notar que o consentimento usualmente está incorporado nas figuras de políticas de privacidade de toda aplicação, como uma maneira de legitimar os modelos de negócios na economia de dados, tendo em vista que é o único meio para utilizar o serviço. Para usufruir do uso de algum aplicativo, o usuário deve aceitar as políticas de uso e consequentemente as de privacidade, impostas a ele. Caso não concorde com estas políticas, o usuário fica impedido de usufruir desse serviço.
> [...] nota-se que o consentimento é usado apenas para dar valor a tais modelos de negócios e não para proteger os dados em si. Esse mecanismo é falho, uma vez que não permite que o usuário goze de sua autodeterminação informativa, pois cabe apenas a ele aceitar ou recusar o serviço utilizado. As políticas de privacidade se instrumentalizam, pois, na forma de um contrato de adesão.

O tema em epígrafe adota um tom mais crítico a partir do momento em que empresas de TIC já apresentam tendências a driblar os termos legais da LGPD no sentido de incorporar, aos seus modelos de negócios, tecnologias cujo funcionamento prescinde do consentimento do titular dos dados, fato este que é estudado por Bioni (2021), em sua doutrina.

Em suas lições, o referido autor preleciona que, rastreadores como *cookies*, os quais se põe a defini-los como "programas de dados gerados com o objetivo principal de identificação do usuário, rastreamento e obtenção de dados úteis a seu respeito, especialmente, baseada em dados de navegação e de consumo [...]" (Martins, 2008, p. 227-228 *apud* Bioni, 2021, p. 16) já possuem outras tecnologias com as quais operam conjuntamente.

O referido autor alude a um estudo realizado pela Universidade de Berkeley, na Califórnia, no sentido de evidenciar o surgimento de novas modalidades de rastreadores que passaram a conviver no ambiente virtualizado com os já bastante presentes *cookies*, chegando ao ponto de substituí-los.

O referido estudo, consistente em navegações simuladas pelos cem sites mais acessados dos Estados Unidos identificou, dentre outros instrumentos de monitoramento, a presença enfatizada de duas novas tecnologias de rastreamento, além daquela alhures já citada: os *flash cookies e HTML5 Web Storage*. No que tange à conceituação do *flash cookie*, define Bioni (2021, p. 149-150):

> Como o próprio nome induz, trata-se de um *tracker* [rastreador] atrelado ao "Adobe Flash", razão pela qual tais rastreadores têm a capacidade de guardar informações sobre vídeos, músicas e outras aplicações dependentes da execução desse programa, além das páginas visitadas, o que é próprio do rastreamento tradicional. Uma outra peculiaridade diz respeito à dificuldade de detectá-lo, já que ele é armazenado em pastas locais do sistema e não na lista de cookies e do histórico da Internet. E, o mais problemático: ele pode reaparecer sempre que for executado o programa da Adobe.

Conceituando o *HTML5 web storage*, Bioni (2021, p. 150) faz uma definição mais simplificada, ao conceituá-lo como "uma evolução do cookie que não expira

automaticamente ao terminar a sessão no navegador, tendo, ainda, uma maior capacidade de armazenamento".

O autor demonstra que, diferentemente dos *cookies*, tais tecnologias exigem mais dispêndio do titular dos dados, tanto para detectá-las quanto para bloqueá-las. Isso sem contar com o fato destas tecnologias serem capazes de se reativar autonomamente através da execução de outras aplicações sem o conhecimento do usuário.

Desta forma, o uso de tecnologias com maiores potenciais de coleta de dados sem que, para tanto, seja necessário o consentimento, tampouco ciência de seu titular, permite o monitoramento onipresente, atemporal e inevitável do usuário de um serviço, o qual, impotente, tem a sua privacidade sorrateiramente desvirtuada.

Ainda neste sentido, Bioni (2021, p. 151) apresenta mais um ferramental de rastreamento, superior às outras tecnologias anteriormente citadas: o *evercookie.*

> O êxtase dessa prática [rastreamento do usuário] é a própria tecnologia *evercookie* que é apelidada de *tracker* [rastreador] zumbi. Por ser o resultado da combinação de inúmeros *trackers*, a coleta dos dados pessoais é quase que perene. Dada essa metamorfose e sobreposição de rastreadores eles continuam a perambular se não há o extermínio de todos eles pelo titular dos dados pessoais. Por exemplo, se o usuário deleta cookies, ele ainda poderá ser rastreado por outros inúmeros *trackers* – *flash cookies*, *E-tags* e assim por diante.

Nos parâmetros atuais, tal fenômeno é recorrente nos provedores de mídias sociais, visto que, inobstante se comportem como redes sociais, também se afiguram como verdadeiros núcleos de coleta e transferência de dados pessoais no contexto da economia digital.

Provedores de mídias sociais são assim conceituados por Crespo (2021, p. 58) como empresas que, ao oferecerem funcionalidades como publicações de textos, fotos e outros arquivos de mídia, permitem que os seus usuários devidamente cadastrados em seu aplicativo ou *site* na internet interajam entre si.

O motivo pelo qual os referidos atores operam como pontos de coleta e transferência de dados se deve pelo fato de que, a fim de oferecer um serviço "gratuito", tais provedores contam com a monetização da coleta e compartilhamento de informações

de seus usuários através de parcerias comerciais firmadas com segmentadores ou *targeters,* os quais são responsáveis por divulgar publicidade direcionada (customizada/personalizada) aos usuários, tudo com fulcro nas informações obtidas pelo seu monitoramento. Aduz Crespo (2021, p. 58-59, grifos do autor):

> [...] são eles [os segmentadores] quem selecionam as mensagens que serão direcionadas para o público-alvo (usuários), de acordo com suas características, interesses ou preferências percebidas dos usuários. Os segmentadores podem querer engajar em interesses comerciais, políticos ou outros. [...] **Os segmentadores podem ter seus próprios *sites* e aplicativos, em que podem integrar ferramentas ou recursos específicos de negócios de mídia social**, como *plugins* ou *logins* sociais ou usando as APIs (*Application Programming Interfaces* ou interfaces de programação de aplicativos) ou *kits* de desenvolvimento de software (SDKs) **oferecidos por provedores de mídia social.** [...]

Tais parcerias comerciais reúnem uma miríade de atores na cadeia econômica dos dados, permitindo assim a instalação de um ecossistema de coleta e processamento de dados, invisível aos usuários do serviço, os quais são monitorados em múltiplas plataformas, independentemente de serem associadas entre si ou não, ante a intensa troca de informações entre ferramentas de monitoramento interligadas.

Ainda neste sentido, de modo a dar ensejo a uma melhor compreensão sobre como o monitoramento do titular dos dados (usuário) ocorre, é mister explorar algumas das principais tecnologias, além das outras supramencionadas no presente estudo, que otimizam o processo de coleta de informações, com destaque para APIs e DMPs como atores da cadeia econômica de dados, quanto às suas capacidades em oferecerem o monitoramento onipresente do titular dos dados a favor dos agentes de tratamento, conforme se verá adiante.

2.2.1 *Application Programming Interfaces* (APIs), *Data Management Providers* (DMPs) e a transcendência das barreiras do mundo digital

As *Application Programming Interfaces* (APIs) ou interfaces de programação de aplicativos correspondem a ferramentas de automação de procedimentos entre aplicações

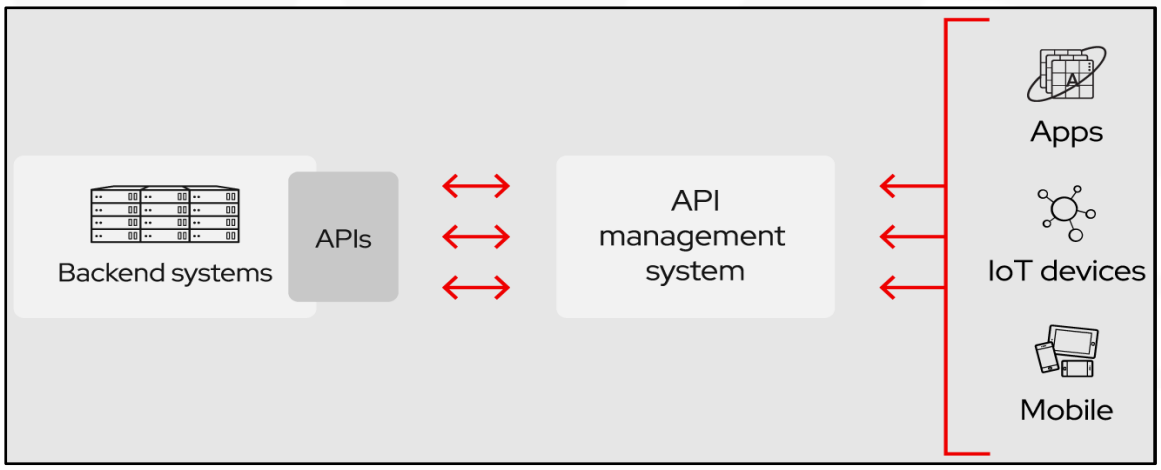
de internet de modo que a resposta que uma aplicação dará ao usuário será baseada diretamente pelo modo de como é estruturada a sua solicitação (Redhat, 2023).

Deste modo, um novo canal de interação entre usuário e agente de tratamento é criado, de modo a otimizar a comunicação entre ambos e consolidar aplicações, de modo a criar uma rede integrada entre serviços e plataformas que aquele primeiro utilize.

Em termos de exemplificação prática, pode-se observar o uso de API com a utilização de um aplicativo de previsão do tempo, pelo qual o dispositivo de uma determinada pessoa que deseja consultar o tempo local de onde se encontre se comunica com os servidores/banco de dados do provedor do serviço (Amazon Web Services, 2023).

Tal comunicação é realizada mediante o compartilhamento de informações que o titular dos dados oferece em sua requisição ao provedor do serviço, como a sua geolocalização e/ou coordenadas geográficas, sob pena de impossibilitar o atendimento de suas requisições. Neste sentido, segue ilustração simplificada, conforme figura 1.

Figura 1 - Como as APIs funcionam?



Fonte: Redhat, 2023

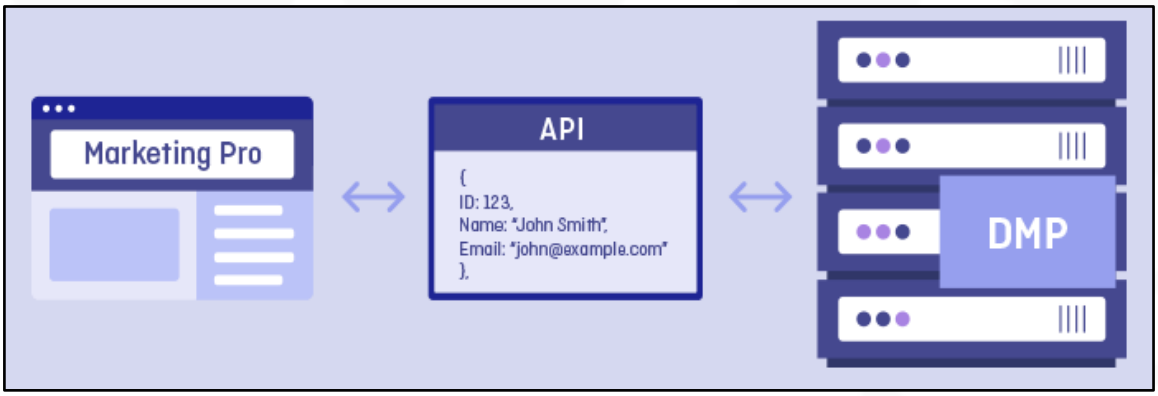
O potencial das APIs, justamente pela sua capacidade de integrar serviços e aplicações em um ecossistema digital, se estende à coleta de dados de múltiplas fontes, sejam estas *online* ou *offline*. Quanto às primeiras, pode-se destacar o histórico de transações, páginas visitadas, *cookies* associados ao usuário, entre outros atributos.

Já no que se refere àquelas últimas, tem-se o exemplo dos pagamentos via comunicação por campo de proximidade (*Near Field Communication* - NFC), operações que prescindem de conexão com a internet para serem efetivadas, haja vista que o fazem por radiofrequência entre aparelhos próximos (Pandey, 2023; Damasceno, 2021). Nestes casos, as informações compartilhadas entre dispositivos são vinculadas a aplicativos bancários, lá ficando armazenadas (Propague, 2022).

Por sua vez, os *Data Management Providers* - DMPs ou Provedores de Gerenciamento de dados correspondem a atores, também inseridos na cadeia da economia dos dados, especializados em processar dados *online* e *offline*, de modo a promover a consolidação, customização e compartilhamento dos dados tratados a outros atores do mercado digital, a exemplo dos já citados segmentadores (Crespo, 2021).

A figura 2 demonstra o fluxograma de interação de dados entre um usuário e um provedor de gerenciamento de dados - DMP, intermediada por uma API.

Figura 2 - A coleta de dados via API para processamento e agregação de um DMP



Fonte: Zawadziński, 2016.

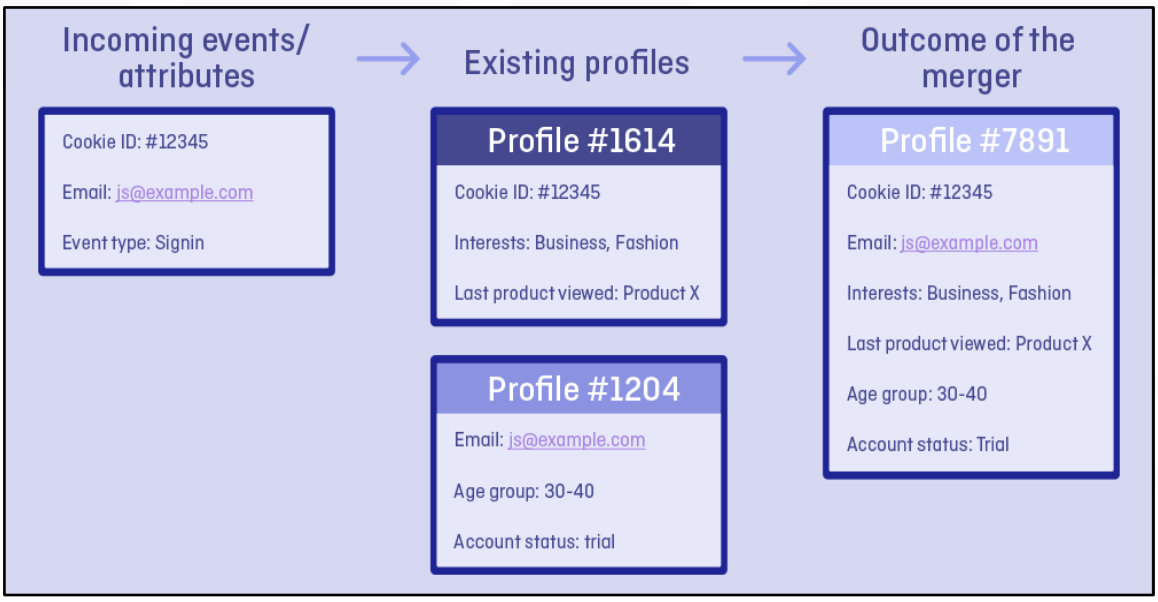
Como ilustrado acima, a API coleta informações do usuário, o qual interage com a plataforma/aplicação (podendo ser uma rede social, um blog, um banco de dados de transações bancárias, etc.) para fins de alimentação do acervo do provedor de gerenciamento de dados - DMP, ao passo que, simultaneamente, ocorre transferência de

informações deste último ao usuário, em resposta às solicitações que este (o usuário) eventualmente fizer conforme o uso de algum serviço.

Uma vez coletados pela API, os dados são agregados pelo DMP de modo a construir perfis de consumo (*profiling*) dos titulares dos dados, processo esse que se norteia essencialmente no sentido de identificar, processar e mesclar informações atreladas a um determinado usuário, não sendo necessário, para os fins deste processo, que as plataformas/serviços dos quais o titular dos dados faça uso pertençam a um mesmo provedor, tampouco que tais recursos devam ser acessados exclusivamente na modalidade *online*, desde que haja, entretanto, um identificador comum entre eles, como os *cookies* ou dados de geolocalização, por exemplo (Zawadziński, 2016).

A figura 3, abaixo, consiste em simplificar o modo de operação dos DMPs.

Figura 3 - *Profile building* mediante consolidação de dados de múltiplas fontes



Fonte: Zawadziński, 2016.

Veja-se acima que a operação consiste em realizar processamento de dados de modo que a recepção de múltiplas fontes de informação (indicada por "*incoming events/attributes*") passa por uma triagem fundada em perfis preexistentes (indicada por

"*existing profiles*") de modo a gerar uma nova informação/perfil através da consolidação de dados não redundantes pelo agregador: o DMP (processo ilustrado na figura por "*outcome of the merger*").

Tais informações do cliente/usuário (*customer data*) são remetidas através de ferramentas a exemplo dos APIs, como intermediadores, para os DMP´s, que qualificam os dados obtidos e os mesclam, eliminando redundâncias (Zawadziński, 2016), processo esse que leva à geração de um novo perfil de consumo atrelado ao usuário, com base nas informações processadas.

Demonstrado o *modus operandi* das referidas tecnologias, é de se notar que a coleta multilateral de dados *online* e *offline* proporcionada pelas APIs, somada à capacidade entrópica dos DMPs em processar dados e compartilhá-los a outros agentes de tratamento de dados, permite a transcendência do monitoramento *online* para o mundo *offline* em face do usuário de modo onipresente e invisível.

A construção de perfis de consumo (*profiling*) fatalmente leva à produção de novas informações correspondentes ao titular dos dados, tornando-as em novos ativos de mercado, ativos estes que, serão lançados a outros atores da cadeia econômica digital, a exemplo dos já mencionados segmentadores, os quais lucrarão com o marketing direcionado baseado na coleta onipresente de dados que, conforme já demonstrado neste tópico, surpassa fronteiras entre o mundo *online* e o mundo *offline*.

Deste modo, provedores de mídias sociais, APIs, DMPs, segmentadores e outros atores da economia dos dados digitais devem se apresentar de modo criteriosamente transparente nos contratos digitais, notadamente no que tange à matéria de circulação dos dados oferecidos pelos seus respectivos titulares no sentido de indicar, sem omissões e de modo simplificado, o modo de como as informações estão sendo tratadas, inclusive quanto aos métodos aplicados por cada ente de tratamento de dados.

Ao contratar com serviços cujo sustento se oriente fundamentalmente pela coleta e processamento de informações, o titular dos dados, por vezes, sequer tem ciência de que as cláusulas dos contratos que firma possam implicar na redução, a níveis ínfimos, de sua privacidade pessoal, especialmente se considerada a sua condição de vulnerabilidade perante empresas de TIC.

É imprescindível a constante revisão de pressupostos éticos em se tratando de tecnologias/atores da cadeia econômica de dados, visto que não se pode, sob pena de desvirtuamento do propósito protecionista da LGPD aos titulares dos dados, impor o uso de novos métodos de coleta e tratamento de dados fulcrados somente na regra do *pacta sunt servanda* e contratos de adesão sem a observância da vulnerabilidade dos titulares.

A autodeterminação informativa é o fundamento concretizado pelo consentimento livre de vícios, nos moldes já estabelecidos pela Lei Geral de Proteção De Dados. Desta forma, ainda no âmbito investigativo do presente artigo, proceder-se-á, a seguir, ao estudo dedutivo dos termos de uso e políticas de privacidade da Meta, visto ser, além de um provedor de mídia social, um polo de integração dos ferramentais já citados até o momento (APIs, DMPs, segmentadores, entre outros).

Visa-se, em última análise, aplicar os preceitos da Lei Geral de Proteção de Dados - LGPD à estrutura dos contratos de adesão que a referida empresa, uma das pioneiras do ramo da TIC, impõe aos seus usuários, ora titulares dos dados.

3 A EMPRESA META: UMA ANÁLISE DOS TERMOS DE USO E POLÍTICAS DE PRIVACIDADE AOS PARÂMETROS DA LGPD

Termos de uso e políticas de privacidade são disposições distintas entre si. A primeira diz respeito ao conjunto de regras relacionadas ao usufruto do serviço pretendido pelo titular, sendo o meio pelo qual o usuário exara o seu “aceite” às disposições às quais se submeterá ao utilizar o serviço, delimitando responsabilidades e direitos entre os contratantes (EJUDI, 2017).

Já a segunda versa especificamente sobre o modo de como os dados serão tratados pelo ente de tratamento, que oferta o serviço, de maneira e explicitar suas práticas e métodos de promoção da segurança entre os contratantes (Sólides, 2021).

Embora distintos em seus conceitos, ambos se apresentam ao titular de modo vinculado, dado que a recusa deste em anuir com os termos de uso importa, também, na rejeição da política de privacidade, indisponibilizando o serviço (Gomes; Bittencourt, 2019).

Analisando-se os termos de uso da Meta, a abordagem se concentra em tratar a respeito da pretensão da referida empresa em utilizar e compartilhar dados pessoais do titular dos dados entre seus parceiros comerciais sem que haja, contudo, especificações concretas direcionadas à identificação de tais parcerias, tampouco nos métodos de tratamento de dados utilizados por cada associado comercial. Assim dispõe a política de privacidade da Meta:

> Coletamos e recebemos informações de parceiros, fornecedores de mensuração, fornecedores de marketing e outros terceiros sobre diversas informações e atividades **dentro e fora dos nossos produtos.**
> [...]
> Nossos parceiros [uma pessoa, empresa, organização ou órgão que usa os nossos Produtos ou se integra a eles para anunciar, comercializar ou fornecer suporte para seus produtos e serviços] também compartilham conosco informações como seu endereço de email, cookies e ID do dispositivo de publicidade [...].
> **Recebemos essas informações independentemente de você ter ou não feito login ou ter ou não uma conta relacionada aos nossos Produtos.**
> Os parceiros também compartilham conosco as comunicações que têm com você caso eles peçam o fornecimento de serviços para a empresa deles, como ajudá-los a gerenciar as próprias comunicações. **Para saber como uma empresa trata ou compartilha suas informações, leia a política de privacidade dela ou entre em contato com a empresa.** (Meta, 2023, n.p, grifos do autor).

Tais disposições, no que diz respeito aos apontamentos sobre o compartilhamento de dados entre parceiros comerciais, refletem um típico padrão seguido por corporações de TIC, que exigem mais informações do que realmente necessitam para assegurar o funcionamento de seus serviços, para fins comerciais.

Ainda se tratando da referida política de privacidade, verifica-se que o contrato da Meta é desfavorável ao usuário no sentido de obstar o exercício do seu direito em saber sobre o modo de como cada parceiro comercial da referida empresa trata seus dados.

Isso porque, conforme a citação alhures grifada, a ele - o usuário - incumbe o ônus de obter tais informações, o que configura sério óbice ao pilar “informação” da diretriz protecionista da LGPD, assim inferido da leitura do art. 5°, XII da Lei Geral de Proteção de Dados, já explicitado neste estudo.

Ressalte-se ainda que, inobstante possível fosse se imaginar que o titular dos dados se debruçasse a ler os termos e condições de cada parceiro comercial, conforme disposto na política da Meta, ainda assim tal ação seria impraticável, visto que não há identificação alguma de tais entidades nas disposições da empresa, que se limita a dar exemplos e breves explicações sobre quem seriam tais atores e o modo de como tratam as informações[4].

Logo, indefinições quantitativas e qualitativas dos contratos digitais referentes à identificação dos agentes e o modo de como estes tratam a informações que lhes são compartilhadas trazem sérias lacunas ao controle do titular dos dados ao fornecê-los aos entes de tratamento, principalmente se considerada a possibilidade de tais agentes/parceiros comerciais terceirizados fazerem uso de tecnologias que prescindem da exaração do seu consentimento para operarem, conforme já demonstrado alhures, neste estudo.

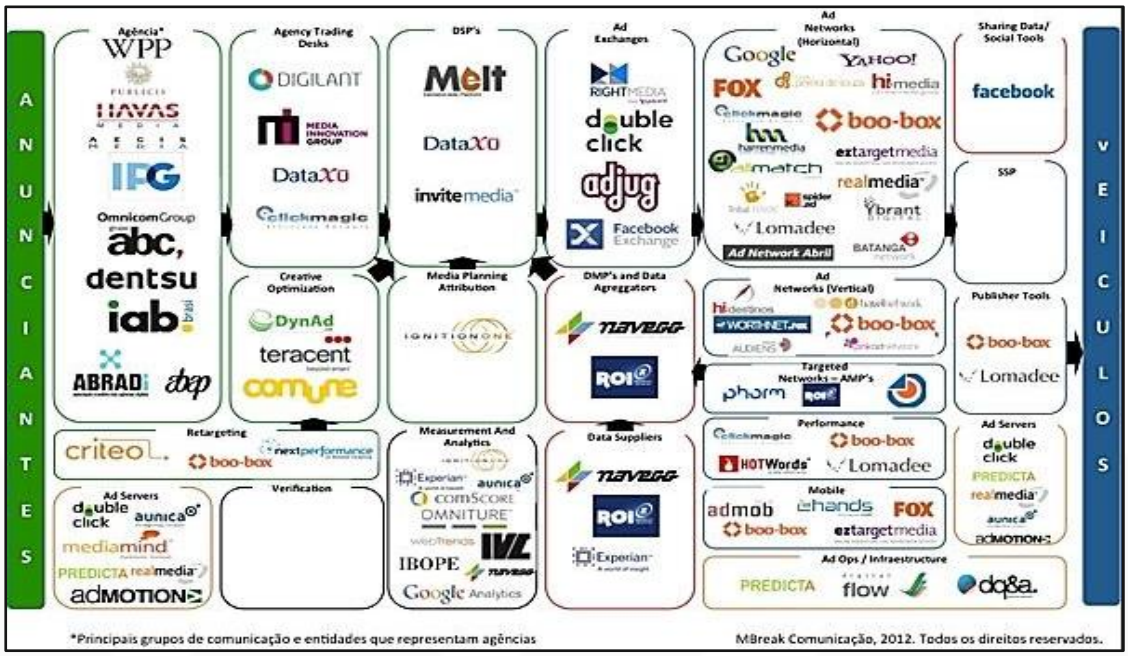
Como exemplo ilustrativo, a figura 4 a seguir demonstra a cadeia digital entre agentes digitais já presente no Brasil em 2012, na qual cada entidade inserida no fluxograma informacional desempenha um papel específico no tratamento de dados.

Veja-se que os anunciantes (coluna verde) contam com diversos intermediadores - grupo ao qual se agregam os DMPs, APIs, provedores de mídias sociais, entre outros – no sentido de coletar, processar e consolidar informações de modo a obterem perfis de consumo para os quais possam veicular publicidade direcionada ao comportamento do público em geral, ora titulares dos dados.

Registre-se que alguns dos entes presentes na tabela já são conhecidos pela sociedade, tais como Google, IBOPE, *Yahoo!* E *Facebook*, bem como outros atores da cadeia digital, os quais interagem entre si com vistas a garantir o trânsito e processamento de informações coletadas dos titulares de dados.

[4] A política de *cookies*, bem como a de privacidade da Meta, embora descrevam o modo de operação quanto aos dados que recebem, pouco aludem sobre o modo de tratamento deles nos domínios de seus parceiros comerciais. Inobstante a política de cookies da plataforma - e tão somente esta política - disponibilize uma série de links pertinentes aos rastreadores/segmentadores aos quais se submete o titular dos dados, o rol apresentado meramente exemplificativo. Isto porque a empresa se restringe a elencar apenas alguns dos rastreadores/segmentadores.

Figura 4 – Rede de publicidade direcionada no mercado brasileiro.



Fonte: Webinsider, 2012.

Conforme o exposto acima, cada ente de tratamento concentra novos círculos de negócios, de modo a gerar uma imprecisão, na perspectiva do titular dos dados, sobre a identidade dos entes de tratamento que compartilham seus dados ou deles se beneficiam. É afirmar, em outras palavras, que, com um único assentimento exarado a um provedor de serviço, o titular dos dados se expõe a diversos outros entes de tratamento de dados cujos métodos carecem de transparência.

Repise-se que, conforme já aludido por Silva (*apud* Vainzof, 2019), no que tange à proteção dos dados exercida pelo titular, esta deve se dar de modo dinâmico, isto é, de modo a se estender aos casos em que os dados fornecidos por um usuário - na condição de titular - em favor de um ente de tratamento, devem ficar sob seu controle ainda que já em domínio de terceiros.

Saliente-se que tais terceiros, dada a sua autonomia de procedimentos e políticas de uso e serviço, conforme se interpreta da política de privacidade da Meta, se equiparam solidariamente a esta empresa à condição de controladores de dados, assim definida pela LGPD nos termos do art. 5°, VI como “pessoa natural ou jurídica, de direito público ou

privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (Brasil, 2018), o que os tornam legalmente responsáveis por eventuais incidentes relacionados à circulação das informações compartilhadas.

A LGPD, mais especificamente em seu art. 9°, é expressa ao dispor sobre os direitos do titular dos dados no que tange às informações sobre o tratamento de dados pessoais e, no mesmo sentido, reforça o inciso VII do art. 18 do mesmo diploma legal[5].

Contudo, inobstante expressa previsão legal da LGPD, a estruturação dos termos de uso e política de privacidade da Meta não se coaduna, em termos de transparência, com as referidas disposições legais, o que se reflete de forma substancialmente prejudicial na manifestação do consentimento do titular dos dados, principalmente no que refere ao aspecto da manifestação informada da sua vontade, dada a imprecisão de agentes e de métodos de tratamento de dados contratados com a Meta.

A imprecisão e opacidade de cláusulas contratuais favorece, assim, um ambiente propício a práticas antiéticas por parte de parceiros comerciais. Frise-se que, a LGPD, notadamente no que diz respeito às suas disposições legais pertinentes ao compartilhamento de dados entre entes de tratamento, é lacônica, deixando de dispor critérios objetivos quanto à referida prática.

Nesse sentido, eventual otimização das disposições legais pertinentes ao saneamento de lacunas legais, com vistas a apurar a precisão da incidência legal do regulamento brasileiro nas relações contratuais digitais se revela imprescindível.

4 CONCLUSÕES TOMADAS

[5] 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: I - finalidade específica do tratamento; [...] **V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade**; **VI - responsabilidades dos agentes que realizarão o tratamento**; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.§ 1º Na hipótese em que o consentimento é requerido, esse **será considerado nulo** caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou **não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.** [...] § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

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;**

Diante dos fatos e fundamentos alhures expostos, é seguro dizer que o modo de obtenção do consentimento dos titulares dos dados se revela precário. Repise-se que inobstante o titular dos dados ainda seja o responsável pela exaração do consentimento, este ainda se encontra impotente diante do fluxo de suas informações.

Isso porque, em que pese o advento da LGPD ter ocasionado uma reforma substancial do *modus operandi* dos entes de tratamento de dados, a realidade prática das relações eletrônicas não oferece o protagonismo nos parâmetros ideais da LGPD.

Mister ressaltar, conforme lições de Crespo (2021), que a LGPD é uma lei de caráter principiológico, isto é, estabelece parâmetros gerais de para que suas disposições legais sejam observadas sem, contudo, prever procedimentos específicos a serem adotados pelos seus tutelados para a consecução de seus fins.

Diferentemente da LGPD, a GDPR - *General Data Protection Regulation* - apresenta critérios mais interventivos na relação contratual digital, com destaque ao que dispõe o seu artigo 14, o qual estabelece que, no que tange aos dados pessoais obtidos por outros meios que não pelo consentimento do titular, os entes de tratamento, *devem* providenciar informações pertinentes: a) à identificação e os detalhes de contato do controlador ou quem assim o represente; b) aos propósitos, bem como as fundamentações legais que justifiquem o tratamento de dados; c) à categoria dos dados coletados, bem como os seus receptores ou categoria de receptores e outras disposições legais. (GDPR, 2016).

Note-se que a referida legislação europeia preserva o seu caráter generalista, visando evitar óbices à economia digital, sem detrimento algum de seu caráter objetivista quanto às suas disposições legais sobre o modo de operação dos entes de tratamento de dados, conforme se observa do parágrafo supramencionado.

Em outras palavras, enquanto a LGPD se estrutura de modo que o dever de um ente de tratamento de dados em prestar informações sobre o seu modo de operação diante do titular se concretiza mediante sua requisição (por provocação), tal obrigação legal se concretiza por imposição expressa (isto é, de ofício), no caso do regulamento europeu, o GDPR.

A economia digital dos dados e as disposições do ordenamento jurídico brasileiro estão fadadas a permanecerem em constante descompasso em matéria de garantias e direitos do titular dos dados como entidade vulnerável, dado que a morosidade em disponibilizar meios de concretização da jurisdição é inerente ao Estado, o que implica em séria desvantagem diante do dinamismo volátil da economia dos dados pessoais.

O advento de novos mecanismos de coleta, processamento e consolidação de dados pessoais (DMPs, APIs, *Cookies*, *Flash Cookies*), conforme já exposto neste presente trabalho, estão preocupantemente alinhados à dispensa do consentimento do titular dos dados.

Frise-se, nesta oportunidade, que qualquer inclinação radical no sentido de elevar burocracias e formalismos legais excessivos a tal nível que se torne inviável a efetivação de relações digitais se mostra nitidamente irrazoável.

Contudo, é igualmente inadmissível que os titulares dos dados, na sua condição de hipossuficientes, permaneçam obstados de exercer, com total integridade, os direitos que lhe são assegurados pela LGPD.

Não se pode, sob pena de violação de princípios inerentes à personalidade - mais especificamente nos aspectos da intimidade e privacidade, bem como ao já aludido fundamento da autodeterminação informativa - elevar a nível absoluto o *pacta sunt servanda* entre entes de tratamento e titulares de dados. Não exaustivamente, consigna Vainzof (2019, p. 24):

> O distanciamento do controle e da autoridade sobre os seus próprios dados, a partir do momento em que o indivíduo não consegue mais identificar quais informações suas são utilizadas, para quais propósitos, e como isso interfere e influencia em sua vida, é um sinal preocupante de tolhimento da autodeterminação informativa, que muitas vezes ocorrerá de forma imperceptível ao titular. [...]

Ainda sobre o distanciamento do titular dos dados quanto a sua autoridade sobre as informações que fornece, Cranor e Mcdonald (*apud* Bioni, 2021) concluíram que grande parte dos usuários de internet desconhecem as opções de privacidade que lhe são

disponibilizadas, os impossibilitando de optarem por suas preferências de privacidade online. Ambas as autoras ainda consignam que:

> [...] consumidores não conseguem se proteger dos riscos que eles não entendem. Encontramos uma lacuna entre o conhecimento que os usuários já possuem e o conhecimento que eles precisariam possuir a fim de fazerem decisões efetivas sobre suas privacidades online. [...] Em termos ideais, usuários deveriam escolher por si mesmos, mas, atualmente, lhes falta conhecimento para tomar decisões de forma informada. (Cranor; Mcdonald, p. 29 *apud* Bioni, 2021, p. 148, tradução nossa).[6]

A condição de vulnerabilidade do titular dos dados deve sempre, em última análise, nortear adoções constantes de diretrizes fiscalizadoras pelo Estado através de suas agências reguladoras no sentido de punir abusos e ilegalidades, além de promover, através de disposições legais mais objetivas, uma proatividade incisiva dos entes de tratamento de dados em atender os seus titulares, sem que, contudo, haja prejuízos ao exercício da economia digital.

5 CONSIDERAÇÕES FINAIS

Na sociedade da informação, dados pessoais se tornaram recursos mercadológicos essenciais à economia digital, marcada pela oferta de serviços baseados na coleta de dados de usuários.

No entanto, o atual modo de estruturação de contratos digitais firmados entre titulares e agentes de tratamento de dados se configura desfavorável àqueles primeiros, haja vista serem eivados de omissões e obscuridades quanto a identidade e métodos de tratamento pertinentes a outros atores da cadeia econômica digital, o que facilita a prática de atos antiéticos, por parte dos entes de tratamento, na coleta de dados dos titulares.

[6] "First and foremost, consumers cannot protect themselves from risks they do not understand. We find a gap between the knowledge users currently have and the knowledge they would need to possess in order to make effective decisions about their online privacy. (...) Ideally, users could choose for themselves but at the present they lack the knowledge to be able to male informed decisions".

A tendência das empresas de TIC à implementação de tecnologias evasivas ao controle do titular dos dados, as quais prescindem do consentimento deste último para operarem - como os já aludidos *evercookies*, bem como outros rastreadores - além do uso de ferramentas de integração de aplicações e coleta multilateral de dados - a exemplo das APIs e DMPs - enseja na transgressão velada das prerrogativas legalmente garantidas aos titulares pela LGPD.

Isso porque as omissões e imprecisões de contratos digitais, os quais, em forma de adesão, reduzem a margem de decisão do titular dos dados pela falta de transparência, principalmente no que se refere ao compartilhamento dos dados do ente contratado para com seus outros parceiros comerciais.

Conclui-se que, inobstante o advento da LGPD, o titular dos dados permanece impotente diante dos entes de tratamento, dado que a opacidade das cláusulas contratuais correspondentes ao compartilhamento de suas informações o torna conivente com as práticas comerciais que lhe são despercebidas. Afinal, não se pode decidir a respeito daquilo que se desconhece.

O distanciamento do jurisdicionado no que diz respeito ao exercício de suas prerrogativas contribui para o enfraquecimento do fundamento da autodeterminação informativa, dada a sua contaminação pela obtenção viciada do consentimento do titular dos dados, por parte dos agentes de tratamento.

De certo que, a LGPD, assim como qualquer outra legislação que lide com a matéria do direito digital, ficará em descompasso com os dinamismos e volatilidades inerentes à sociedade da informação, inobstante o seu caráter predominantemente principiológico tivesse sido concebido pelo legislador justamente com o propósito de evitar obsolescências do texto legal.

Deste modo, de forma a evitar eventuais complicações relacionadas a sua eficácia no mundo fático, é mister elaborar a seguinte questão: Como ponderar os ditames legais da LGPD sem inviabilizar a economia digital?

Resposta para tal inquirição poderia ser encontrada na implementação, por parte da LGPD, de parâmetros já adotados na sua legislação paragonada GDPR, visto esta

última ser mais ingerente nas relações digitais entre titulares e entes de tratamento de dados.

Isso se deve em virtude de o regulamento europeu pressupor (por imposição legal expressa), por parte dos entes de tratamento de dados, a disponibilização de meios hábeis pelos quais o titular possa exarar sua manifestação de consentimento livre de vícios quanto sua liberdade, tampouco sua autodeterminação informativa, dado que a relação contratual digital junto ao ente de tratamento de dados será firmada e delimitada através do seu assentimento.

Em última análise, o saneamento legal da LGPD com vistas a lhe aferir maior objetividade em um processo de transição de caráter principiológico-subjetivo em favor de um porte pragmático-objetivo contribuiriam substancialmente ao seu propósito protecionista do titular dos dados, dada a sua condição de vulnerabilidade e, ao mesmo tempo, harmonizariam com a economia dos dados digitais.

REFERÊNCIAS

AMAZON WEB SERVICES. **O que é uma api?** Disponível em: https://aws.amazon.com/pt/what-is/api/. 2023. Acesso em: 19 set. 2023.

ARAÚJO, Sidney. **NFC ou MST:** qual a melhor tecnologia de pagamento via celular? Mobile transaction, 05 jul. 2019. Disponível em: https://br.mobiletransaction.org/nfc-mst-qual-melhor/**.** Acesso em: 15 set. 2023.

BIONI, Bruno. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021.

BRASIL. Lei nº 13.709/18. **Lei Geral de Proteção de Dados Pessoais (LGPD**). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 maio 2023.

BRASIL. Congresso Nacional. **Projeto de lei 4060/2012**. Brasília, DF: portal da Câmara, 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 19 ago. 2023

CRESPO, Marcelo. A publicidade digital e a LGPD: insights sobre o modelo de negócios e como proteger dados pessoais**.** ***in*****:** DE LIMA, Ana; CRESPO, Marcelo; PINHEIRO, Patrícia (coord.). **LGPD aplicada.** São Paulo: Atlas, 2021.p. 54-68.

DAMASCENO, Luciana. **O que é NFC e como ele funciona para pagamentos?** Mobile transaction, 03 out. 2021. Disponível em: https://br.mobiletransaction.org/o-que-e-pagamento-via-nfc/. Acesso em 15 set. 2023.

EJUDI SOLUÇÕES JURÍDICAS. **Termo de uso**: conheça seus requisitos e sua finalidade. 24 nov. 2017. Disponível em: https://ejudi.com.br/termo-de-uso-finalidade/. Acesso em: 17 out. 2023.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council**. Regulation (EU), 2016. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en. Acesso em: 29 abr. 2023.

FACEBOOK. **Política de privacidade**. 2023. Disponível em: https://pt-br.facebook.com/privacy/policy/?entry_point=facebook_page_footer. Acesso em: 28 maio 2023.

FACEBOOK. **Política de *cookies***. 2022. Disponível em: https://www.facebook.com/privacy/policies/cookies/?entry_point=cookie_policy_redirect&entry=0. Acesso em: 27 maio 2023.

FERREIRA, Ricardo *et a*l. **Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia.** Portal migalhas, 04 jun. 2018. Disponível em: https://www.migalhas.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia. Acesso em: 19 ago. 2023.

FIA BUSINESS SCHOOL. **GDPR [guia completo]:** tudo que você precisa saber sobre a Lei. 03 jan. 2019. Disponível em: https://fia.com.br/blog/gdpr/#:~:text=A%20primeira%20proposta%20para%20o,somente%20em%20maio%20de%202018. Acesso em: 19 ago. 2023.

GOMES, Évelyn Vieira; BITTENCOURT, Izabella Alves Jorge. O Consentimento nas leis de proteção de dados pessoais: Análise do regulamento geral sobre a proteção de dados Europeu e da lei Brasileira 13.709/2018. *In*: POLIDO, Fabrício; ANJOS, Lucas; BRANDÃO, Luíza (orgs.). **Políticas, Internet e Sociedade**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2019. Disponível em: http://bit.ly/35hiqms. Acesso em: 15 maio 2023.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro:** contratos e atos unilaterais. 16. ed. São Paulo: Saraiva Educação, 2019. v. 3.

INSTITUTO PROPAGUE. **O que é nfc?** 29 jun. 2022. Disponível em: https://institutopropague.org/pagamentos/nfc-o-que-e-e-como-essa-tecnologia-facilita-os-pagamentos/. Acesso em: 13 out. 2022.

PANDEY, Prachi. **Offline Digital Payments**: Meaning, Advantages, How it Works and more. SabPaisa. 30 jun. 2023. Disponível em: https://sabpaisa.in/blog/offline-digital-payments/#:~:text=Ans%3A%20Examples%20of%20offline%20digital,even%20without%20an%20internet%20connection. Acesso em: 15 set. 2023.

REDHAT. **O que é api?** 19 jan. 2023. Disponível em: https://www.redhat.com/pt-br/topics/api/what-are-application-programming-interfaces. Acesso em: 15 set. 2023.

SANT´LAGO, Marcelo. **O que esperar do mercado de display media e RTB no Brasil em 2013?** Webinsider, 18 dez. 2012 Disponível em: https://webinsider.com.br/2012/12/18/o-que-esperar-do-mercado-de-display-media-e-rtb-no-brasil-em-2013/. Acesso em: 25 maio 2023.

SÓLIDES. **O que é Política de Privacidade, como fazer e sua relação com a LGPD**. 10 set. 2021. Disponível em: https://blog.solides.com.br/o-que-e-politica-de-privacidade/. Acesso em: 15 out. 2023.

VAINZOF, Rony. Disposições preliminares. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2 ed. São Paulo: Thomson Reuters Brasil, 2019. *E-book*.

ZAWADZIŃSKI, Maciej. **How Does Data Collection Work in a DMP?** Piwik Pro, 31 out. 2016. Disponível em: https://piwik.pro/blog/data-collection-dmp/. Acesso em: 14 set. 2023.