



## BREVES CONSIDERAÇÕES ACERCA DA MONETIZAÇÃO DE DADOS PESSOAIS NA ECONOMIA INFORMACIONAL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Jéssica Andrade Modesto\*

### RESUMO:

Na economia informacional os dados pessoais são constantemente monetizados. Diante disso, buscou-se investigar se essa prática é legal, bem como quais serão os impactos que a Lei Geral de Proteção de Dados provocará nessa atividade. Para tanto, foi realizada uma pesquisa bibliográfica/documental sobre o tema. Concluiu-se que a monetização de dados pessoais é lícita, mas deve seguir os limites impostos pelo ordenamento jurídico. Nesse sentido, a LGPD trouxe importantes diretrizes a serem seguidas pelas organizações, se estas não quiserem sofrer sanções administrativas, além de estarem sujeitas à responsabilização civil.

**Palavras-chave:** Monetização; Dados Pessoais; Economia Informacional; Lei Geral de Proteção de Dados Pessoais; Lei nº 13.709/2018.

### BRIEF CONSIDERATIONS ABOUT MONETIZATION OF PERSONAL DATA IN THE INFORMATION ECONOMY ACCORDING TO THE GENERAL PERSONAL DATA PROTECTION LAW

### ABSTRACT:

In the information economy, personal data are constantly monetized. Therefore, we sought to investigate if this practice is legal, as well as what will be the impacts that the General Data Protection Law will have on this activity. For this, a bibliographic/documentary research on the theme was carried out. It was concluded that the monetization of personal data is lawful, but it must follow the limits imposed by the legal system. Thus, the LGPD brought important guidelines to be followed by organizations, if they do not want to suffer administrative sanctions, in addition to being subject to civil liability.

**Keywords:** Monetization; Personal data; Informational Economy; General Law on Protection of Personal Data; Law n. 13.709/2018.

## 1 INTRODUÇÃO

Atualmente, a economia cada vez mais é marcada por modelos de negócios que utilizam os dados pessoais para as mais diversas finalidades. Na era do *big data*, a ordem é

---

\* Mestranda em Direito Público pela Universidade Federal de Alagoas. Graduada em Direito pela Universidade Federal de Alagoas. Advogada. Servidora Pública Federal. Orcid: <https://orcid.org/0000-0002-2626-5088>. E-mail: [jessicaandrademodesto@hotmail.com](mailto:jessicaandrademodesto@hotmail.com)



coletar o máximo de dados que se conseguir antes mesmo de saber se tais informações serão úteis. Isso porque esses dados podem ser tratados de forma a auxiliar a tomada de decisão, bem como serem submetidos a procedimentos que podem agregar bastante valor às organizações empresárias.

Dessa forma, não raramente essas organizações criam artimanhas para coletarem os dados pessoais, seja obrigando os indivíduos a fornecerem uma quantidade demasiada e desnecessária de dados para poderem concluir uma relação contratual, seja coletando por meio de tecnologias da internet como os *cookies*, o que muitas vezes acontece sem o conhecimento do titular desses dados.

Também são frequentes as situações em que os indivíduos fornecem seus dados pessoais para poderem utilizar serviços “gratuitos”. São diversos serviços de grande utilidade fornecidos, principalmente na internet, e que podem ser usufruídos sem uma contrapartida pecuniária, no entanto, na imensa maioria das vezes, a utilização dessas aplicações exige que os usuários compartilhem seus dados com as organizações provedoras de tais serviços. Os chamados “gigantes da tecnologia”, como o *Google* e o *Facebook*, são exemplos disso.

Assim, em razão das facilidades que essas organizações oferecem à sociedade, as pessoas toleram fornecer seus dados pessoais em troca desses serviços. Hoje, é impossível imaginar um mundo no qual os indivíduos não queiram utilizar o mecanismo de busca do Google, redes sociais ou até mesmo *smartphones*, que coletam dados como informações de geolocalizações mesmo com a desabilitação no dispositivo da opção que permite a coleta dessas informações.<sup>123</sup>

Em contrapartida aos serviços oferecidos, as organizações coletam uma imensa quantidade de nossos dados pessoais<sup>4</sup>. Mas por que oferecer um serviço em troca dessas

<sup>1</sup> Um estudo recente conduzido por Douglas C. Schmid, professor de Ciência da Computação da Universidade de Vanderbilt demonstrou que um aparelho inativo rodando o sistema operacional Android remete informações de geolocalização ao Google cerca de 340 vezes por dia, o que representa uma média de 14 envios por hora. (TSUKAYAMA, 2018).

<sup>2</sup> O Google reconheceu que o histórico de localizações dos usuários do Android são enviados aos seus servidores mesmo com a opção desabilitada, de modo que esse compartilhamento só é efetivamente encerrado quando o usuário acessa a sua conta no Google e altera as configurações de privacidade na guia “Web andAppActivity”. (NAKASHIMA, 2018).

<sup>3</sup> No suporte de ajuda do Google é possível encontrar a seguinte informação: “Mesmo depois que você desativar o Histórico de localização, alguns dados de local poderão continuar a ser salvos em outras configurações, como na Atividade na Web e de apps, quando você usar outros serviços, como a Pesquisa Google e o Maps.” (GOOGLE, 2019a).

<sup>4</sup> O site do Google, por exemplo, informa quais dados dos usuários são coletados:



informações? Qual o valor dos dados pessoais para as organizações empresárias? A monetização desses dados é legalmente possível? Quais os impactos que a Lei Geral de Proteção de Dados na atividade de monetização de dados pessoais?

O presente trabalho se propõe a responder essas questões, partindo-se da hipótese de que a monetização de dados pessoais é legal, entretanto, deve observar parâmetros éticos e jurídicos. Para tanto, será realizada uma pesquisa bibliográfica/documental sobre o tema, bem como serão feitas algumas breves considerações acerca da economia da informação e da monetização de dados pessoais nesse cenário. Em seguida, analisar-se-ão as disposições da LGPD que deverão ser observadas nesse tipo de tratamento de dados.

## **2 ECONOMIA DA INFORMAÇÃO E MONETIZAÇÃO DE DADOS**

O desenvolvimento tecnológico nos coloca diante do que Manuel Castells denomina de informacionalismo ou capitalismo informacional, o qual tem a informação como a base material e tecnológica da atividade econômica e da organização social (CASTELLS, 1999).

Nesse contexto, uma imensa quantidade de informação é produzida a cada segundo, especialmente quando se fala em conectividade, internet e redes sociais, a exemplo de *sites* visitados, tempo gasto com a visitação a esses *sites*, preferências de compras, localização, entre outros, existindo um fluxo constante e inesgotável de informação, que é coletado por

---

Coletamos informações sobre sua atividade em nossos serviços e usamos tal informação para recomendar um vídeo do YouTube de que você pode gostar, por exemplo. As informações de atividades que coletamos podem incluir o seguinte: termos que você pesquisa; vídeos que você assiste; visualizações e interações com conteúdo e anúncios; informações de voz e áudio quando você usa recursos de áudio; atividade de compra; pessoas com quem você se comunica ou compartilha conteúdo; atividades em sites e apps de terceiros que usam nossos serviços; histórico de navegação do Chrome que você sincronizou com a Conta do Google.

Se você usa nossos serviços para fazer e receber chamadas ou enviar e receber mensagens, podemos coletar informações de registro de telefonia, como o número do seu telefone, número de quem chama, número de quem recebe, números encaminhados, horário e data de chamadas e mensagens, duração das chamadas, informações de roteamento e tipos de chamadas. [...]

Em algumas circunstâncias, o Google também coleta informações sobre você de fontes de acesso público. Por exemplo, se seu nome aparecer em um jornal local, o mecanismo de pesquisa do Google poderá indexar esse artigo e exibi-lo para outras pessoas, se elas pesquisarem pelo seu nome. Também podemos coletar informações sobre você de parceiros confiáveis, incluindo parceiros de marketing que nos fornecem informações sobre clientes em potencial para nossos serviços comerciais e parceiros de segurança que nos fornecem informações para proteção contra abuso. Também recebemos informações de anunciantes para fornecer serviços de publicidade e pesquisa em nome deles.

Usamos várias tecnologias para coletar e armazenar informações, incluindo cookies, tags de pixel, armazenamento local como armazenamento do navegador da Web ou caches de dados de aplicativos, bancos de dados e registros do servidor (GOOGLE, 2019b).



organizações empresárias variadas e possuem destinação, em muitos casos, não informada (CARVALHO, 2018, p. 381).

Dessa forma, a economia, aproveita-se do fenômeno do *big data*, fazendo surgir novos modelos de negócios, que coletam e tratam estes dados. Essa nova economia se caracteriza por ser um ambiente no qual ocorrem rápidas transformações e surgem novos tipos de negócios, mas, a principal característica é a quantidade de informações disponíveis para processamento (COHEN, 2002, p. 26). Não há mudanças nas regras gerais da economia, a mudança que se verifica na economia está na forma em que a informação é utilizada, razão pela qual alguns entendem que o termo mais apropriado para designar essa nova economia é “economia da informação” (COHEN, 2002, p. 8).

Assim, na economia da informação as informações pessoais são tidas como o novo petróleo e se tornam verdadeiros ativos dessas organizações (VITAL, 2018, p. 01). O conceito de dado pessoal pode ser entendido como os fatos, comunicações e ações que se referem a um indivíduo identificado ou identificável (MENDES, 2014, p. 55-56).

Em outras palavras, dado pessoal é todo dado relacionado a uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (Art. 4º, RGPD. UNIÃO EUROPEIA, 2016).

Dito isso, o avanço tecnológico abre caminho para a monetização de informações e essa prática é um dos principais componentes dos modelos de negócios modernos (ADJEI, 2015, p. 01). Situação ilustrativa da importância dos dados em relação às receitas das organizações é o caso da Caesars Entertainment Operating Co., que entrou com pedido de falência em 2015, tendo como principal ponto de disputa seu programa de fidelidade dos clientes, o *Total Rewards Loyalty Program*:

Repleto de Big Data e construído durante os últimos 17 anos, os rumores é de que ele tem os dados de mais de 45 milhões de clientes. Os credores avaliam que esses dados valem cerca de U\$\$ 1 bilhão – um número e tanto. Ele ultrapassa o valor de qualquer bem físico da Caesar em Las Vegas, o que dá uma boa perspectiva em relação ao valor dos dados. Também dizem que o programa equivale a 17% do valor total de todos os ativos operacionais da Caesar’s (TODD, 2015).





Pelo caso relatado acima é possível concluir que os dados pessoais representam atualmente uma importante fonte de receitas para os empresários e, nesse sentido, também quando ocorrem fusões e aquisições de organizações os dados podem ser apontados como um dos principais ativos buscados, mais até do que pessoal, propriedade intelectual e espaço físico, tal qual aconteceu na aquisição do *site Linda.com* pelo *LinkedIn* (TODD, 2015).

O conceito de monetização possui várias dimensões, não sendo limitado ao âmbito das informações pessoais e internet, entretanto, nesse contexto, a monetização de informações seria a transformação de coisas que, a princípio, não possuem nenhum valor agregado, em coisas com algum valor, de modo que as informações pessoais podem ser utilizadas como um instrumento para facilitar transações e, ainda, como o próprio objeto dessas transações (ADJEI, 2015, p. 01).

A título de exemplo, numa mesma operação é possível observar essas duas facetas da utilização das informações. Determinada organização pode coletar e tratar os dados de seus clientes e, a partir dessas informações, personalizar o serviço prestado ou o produto vendido a esses mesmos clientes, assim as informações são utilizadas como um meio para facilitar e aprimorar as transações dessa organização. Por outro lado, esse mesmo empresário pode coletar e tratar os dados de seus clientes e repassá-los a um terceiro, mediante contraprestação, de modo que as informações tornam-se o próprio objeto da transação.

Uma descrição prática do funcionamento da monetização de dados pessoais é fornecida por Rochfeld, a partir de um questionamento: “Como é possível transformar dados pessoais em valor?”:

Eis um exemplo que permite uma imersão na economia subterrânea da segmentação e da predição, a partir do processamento de dados pessoais, para direcionar a visualização de informações dirigidas por meio de interfaces escondidas dos nossos computadores. As informações sobre as preferências e as preocupações do usuário são armazenadas no disco rígido do computador através dos *cookies* de conexão ou de navegação. Eles são pequenas sequências de códigos, armazenados à medida que as visitas são feitas pelos internautas em sítios eletrônicos variados da Internet. Posteriormente essas informações são ativadas quando o usuário navega: os *cookies* fornecem detalhes dessas visitas aos parceiros de agências de publicidade especializadas, responsáveis pela gestão desses dados coletados. As agências celebram contratos com os sítios eletrônicos para essa finalidade. Em seguida, as agências analisam e adaptam de forma extremamente rápida (em centésimos de segundo) a publicidade destinada especialmente à pessoa visada. Assim, um comerciante ou prestador de serviço (ou, mais precisamente, a agência que administra sua conta de publicidade) torna-se capaz de fornecer (ou deveria sê-lo), em um tempo muito curto, uma lista específica de produtos e serviços relacionados com as visitas anteriores e os interesses dos internautas, de forma direcionada. Na



prática, como evidenciam os números anteriormente mencionados, os dados pessoais são assim monetizados, cedidos, revendidos, transferidos e terceirizados dentro e fora da União Europeia, enquanto novos atores – *dataminers*, *databrokers*, analistas, especialistas em algoritmos, etc. – tornam-se centrais na economia global. (ROCHFELD, 2018, p. 63-64).

O caminho, como visto, é se utilizar dos dados coletados para vender produtos ou serviços de forma mais direcionada ao usuário específico, aperfeiçoando os relacionamentos entre os empresários e seus clientes, bem como compartilhar esses dados com terceiros que busquem ampliar a sua base de dados para além da sua própria carteira de clientes.

Assim, abrem-se novas possibilidades de remuneração para as organizações, seja por meio do aprimoramento de seus próprios negócios ou por meio da venda desses dados a terceiros. Dessa forma, existem duas abordagens para a monetização de dados, uma interna e uma externa, sendo interna aquela que visa a transformar os dados em inteligência capaz de alavancar resultados, e a externa aquela que transforma os dados pessoais em um produto com relevância e valor de mercado, de modo a se apresentar como uma nova fonte de receita para o negócio (YAMAGATA, 2017).

Nesse sentido, as organizações utilizam as informações de diversas formas e de acordo com as estratégias almejadas pelo empresário, tais como redução de custo, criação de valor, interconectividade, inovação, redução de risco e diferenciação de produto. “Usa-se a informação para saber como agem os clientes, para controlar estoques, aumentar a produtividade etc. A informação pode ser um ativo, ou simplesmente uma ferramenta de suporte à decisão”<sup>5</sup> (COHEN, 2002, p. 28).

Dessarte, monetização de informações pessoais é o processo pelo qual ocorre a transformação de dados em mercadorias que gerem interesse de terceiros e sobre os quais haverá rentabilidade para o responsável pela sua coleta e/ou tratamento (ADJEI, 2015, p. 02).

Como visto, isso pode ser bastante vantajoso, tendo em vista que a publicidade é apontada como a principal fonte de receita de grandes corporações como o *Google* e o *Facebook*. Para se ter uma ideia, estima-se que a pandemia do COVID-19 ocasione uma perda para essas corporações de US\$ 44 bilhões em receita de publicidade no ano de 2020 (O ESTADO DE SÃO PAULO, 2020). Em 2019, as receitas de publicidade do Google oriundas somente do *YouTube* atingiram US\$ 15,15 bilhões (SANTINO, 2020).

<sup>5</sup> COHEN, Max E. Alguns aspectos do uso da informação na economia da informação. *Ciência da Informação*, v. 31, n. 3, 2002. Disponível em: [http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci\\_abstract&tlng=pt](http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt). Acesso em: 02 abr. 2020, p. 28.





Nesse cenário, a utilização dos dados pessoais como verdadeiros insumos na realização de novos negócios tem a grande vantagem de estas matérias primas serem renováveis e crescentes diariamente. Desse modo, monetizar os dados pessoais significa “promover o desenvolvimento econômico, construindo negócios rentáveis” (CARVALHO, 2018, p. 76).

A denominada “economia da informação”, portanto, está provocando mudanças na forma como os empresários praticam seus negócios, de modo que se verificam profundas transformações na forma de as organizações operarem e na necessidade de se repensarem os fundamentos da estratégia empresarial, transformações essas que se apresentam como novas formas de negócios, comunicação e interação, diminuindo os obstáculos criados pelo tempo e pelo espaço (COHEN, 2002, p. 26).

No entanto, é importante frisar que o desenvolvimento desse novo modelo de negócios traz ao centro do debate a questão da violação à privacidade dos indivíduos cujos dados pessoais são utilizados como insumo, de modo que aos governos nacionais põe-se o desafio de sopesar desenvolvimento econômico e proteção à privacidade, buscando instrumentos capazes de permitir crescimento econômico e minimizar os impactos sobre a privacidade (ADJEI, 2015, p. 01).

Atualmente, o direito à privacidade tem sua compreensão ampliada em razão de a evolução das formas de divulgação e apreensão de dados pessoais ter expandido as possibilidades de violação da esfera privada, máxime pelo acesso não autorizado de terceiros a esses dados.

Dessa feita, a tutela da privacidade alarga seus contornos tradicionais de “direito a ser deixado só” ou “direito de ser deixado em paz” para apresentar-se também como o direito de manter o controle sobre as próprias informações (SCHEREIBER, 2014, p. 137). Dentro desse contexto, o direito à proteção de dados pessoais é reconhecido como uma espécie do direito fundamental à privacidade e alicerça-se na autodeterminação informativa, isto é, sinteticamente, no direito de cada indivíduo decidir quando e como dispor de suas informações (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 47).

De fato, são diversos os exemplos de violação à privacidade dos indivíduos decorrentes da monetização de dados pessoais, tais como organizações empresárias que costumam coletar todo tipo de informação, muitas das quais não são necessárias para a



finalidade de suas atividades. Ademais, não raramente o indivíduo nem chega a saber que seus dados estão sendo enviados e armazenados por uma dessas organizações.

Além disso, muitas vezes não há transparência no uso dos dados pessoais coletados, os quais frequentemente são compartilhados, gratuita ou onerosamente, com os chamados “parceiros” das organizações, tudo isso sem o consentimento da pessoa a quem estas informações se referem. Ainda, não se pode esquecer as situações em que o indivíduo não consegue ter acesso a tais informações, nem pedir a correção de seus dados e, principalmente, vê negada a possibilidade de apagamento dos seus dados coletados, os quais, de maneira frequente, são mantidos nos servidores das organizações mesmo quando o relacionamento do indivíduo com esta é encerrado e a conta de usuário é excluída.

Assim, percebe-se que muitos empresários costumam agir como se os dados pessoais coletados fossem bens dos quais se apropriaram e, por conseguinte, podem ser usufruídos irrestritamente.

Contudo, tem crescido cada vez mais a preocupação com a privacidade das pessoas em meio aos novos modelos de negócio que surgem na nova economia. Estas preocupações levam à criação de legislação específica sobre a tutela dos dados pessoais, como a Lei nº 13.709/2018, no Brasil, a chamada Lei Geral de Proteção de Dados Pessoais – LGPD, ainda em *vacatio legis*.

### **3 IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA ATIVIDADE DE MONETIZAÇÃO DE DADOS PESSOAIS**

A Lei Geral de Proteção de Dados Pessoais certamente implicará nas atividades de monetização dessas informações. Nesse sentido, a LGPD traz uma série de disposições que devem ser observadas pelos agentes de tratamento em todo o processo de utilização de informações, destacando-se, para o presente estudo, o estabelecimento das hipóteses em que o tratamento de dados é legal, os princípios a serem seguidos em todos os procedimentos, bem como os direitos dos titulares dos dados.

No que diz respeito às hipóteses em que a lei autoriza o tratamento de dados pessoais, o artigo 7º prevê que o referido tratamento somente poderá ser realizado mediante o fornecimento do consentimento pelo titular ou, independentemente do consentimento, no caso





de situações específicas como quando necessário ao cumprimento de obrigação legal ou à execução de políticas públicas.

Por sua vez, consentimento é definido como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5º, XII), de modo que as autorizações genéricas para o tratamento de dados pessoais são nulas, cabendo ao controlador o ônus da prova de que o consentimento fora obtido em conformidade com a LGPD.

Além disso, a Lei dispõe que, em se tratando de dados pessoais sensíveis<sup>6</sup>, o consentimento deverá ser fornecido de forma específica e destacada (art. 11). E, em se tratando do tratamento de dados pessoais de crianças e de adolescentes, este deverá ser realizado em seu melhor interesse, com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, bem como os controladores não deverão condicionar a participação desses indivíduos em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade (art. 14).

Outrossim, o consentimento 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.

Dessarte, como regra, a Lei nº 13.709/2018, não proíbe a monetização de dados pessoais, entretanto, impõe vários limites a tal prática.

Assim, o primeiro ponto a ser levado em consideração é que o consentimento do titular dos dados adquire bastante relevo nessa discussão. Isso porque, como visto, ausente qualquer hipótese legal que autorize o tratamento de dados, este somente poderá ser realizado se o titular tiver consentido.

Nesse sentido, as organizações que intencionem coletar dados pessoais devem se adequar a esse quadro normativo, embutindo em seus sistemas soluções que assegurem ao

---

<sup>6</sup> Dados pessoais são aqueles mais suscetíveis de serem utilizados com finalidades discriminatórias ou lesiva, razão pela qual merecem ser especialmente protegidos contra os riscos de sua circulação, estabelecendo-se regras mais rigorosas para sua coleta, tratamento e armazenamento. (RODOTÀ, 2008, p. 96). No Brasil, o artigo 5º, II, da LGPD dispõe que são sensíveis os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.



titular dos dados a possibilidade de manifestar inequivocamente seu consentimento de maneira livre e informada. Outrossim, aquele que desejar coletar dados pessoais deverá informar ao titular a forma, a duração e a finalidade do tratamento dos dados, além dos riscos a serem suportados pelo titular.

Também, em caso de alteração na finalidade específica do tratamento dos dados, o titular deverá ser informado, com destaque de forma específica do teor das alterações, de modo que, nos casos em que o seu consentimento é exigido, poderá revogá-lo caso discorde da alteração. Por fim, deve-se garantir que o consentimento possa ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

Dessa forma, observa-se que as organizações não mais poderão coletar dados pessoais sem que o titular desses dados saiba quais informações estão sendo coletadas e para qual finalidade os dados serão utilizados.

Destaca-se, ainda, que não basta a manifestação inequívoca e informada pelo titular, pois, como visto, a Lei nº 13.709/2018 exige que o consentimento seja qualificado como livre. Isso posto, esse ponto levantará muitos questionamentos.

Pode ser considerado livre o consentimento fornecido na hipótese de um serviço que se diz ser ofertado gratuitamente, mas que exige o fornecimento de dados pessoais para que seja utilizado, isto é, um serviço a que o indivíduo somente poderá ter acesso se consentir com a coleta e até com o compartilhamento de seus dados pessoais?

Nessa situação pautada pela lógica do “tudo ou nada”, em que ou o titular consente em fornecer seus dados pessoais ou não pode utilizar o serviço, não há verdadeiramente uma liberdade de escolha. Dessa forma, com a vigência da Lei nº 13.709/2018, a Autoridade Nacional de Proteção de Dados deve avaliar se o consentimento obtido em tal hipótese é ou não válido nos termos da LGPD.

Acerca disso, o Grupo de Trabalho do Artigo 29<sup>7</sup>, ao tecer suas orientações relativas ao consentimento na acepção do Regulamento Geral de Proteção de Dados da União Europeia, entende que o consentimento nessa situação não é livre e, portanto, não é válido:

O elemento «livre» implica uma verdadeira escolha e controlo para os titulares dos dados. Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido. Se o

<sup>7</sup> Este Grupo de Trabalho é um órgão consultivo europeu independente em matéria de proteção de dados e privacidade, o qual foi instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE.





consentimento estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que não foi dado livremente. Assim sendo, não se considera que o consentimento foi dado de livre vontade se o titular dos dados não o puder recusar nem o puder retirar sem ficar prejudicado. A noção de desequilíbrio entre o responsável pelo tratamento e o titular dos dados também é tida em consideração no RGPD.

[...] Em termos gerais, qualquer elemento que constitua pressão ou influência desadequada sobre o titular dos dados (que se pode manifestar de formas muito diversas) e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido.

[Exemplo 1] Uma aplicação para telemóvel de edição de fotografias solicita aos utilizadores que ativem a localização por GPS para fins de prestação dos serviços. A aplicação também os informa de que utilizará os dados recolhidos para efeitos de publicidade comportamental. Nem a geolocalização nem a publicidade comportamental em linha são necessárias para a prestação do serviço de edição de fotografias, indo além da concretização do serviço principal prestado. Uma vez que os utilizadores não podem utilizar a aplicação sem darem o seu consentimento para estes efeitos, o consentimento não pode ser considerado livre (GRUPO DE TRABALHO, 2017).

Uma vez que a lei brasileira de proteção de dados pessoais sofreu forte influência do RGPD, é possível que a Autoridade Nacional de Proteção de Dados Pessoais adote semelhante interpretação.

E se o serviço, além de oferecer a versão “gratuita” do serviço – cuja contrapartida são os dados pessoais dos usuários –, também oferecer uma versão *premium*, pela qual o usuário paga um determinado valor pela utilização do serviço? Nessa situação, permite-se que o usuário realmente escolha entre pagar pela utilização do serviço ou fornecer suas informações pessoais para que sejam monetizadas pela organização empresária, inclusive com a possibilidade de cessão onerosa de tais dados. Verifica-se que o consentimento do titular pode ser qualificado como livre, nesse caso.

Ademais, a LGPD, em seu artigo 6º, dispõe que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios da: a) finalidade do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular; b) adequação do tratamento com as finalidades informadas ao titular; c) limitação do tratamento ao mínimo necessário para a realização de suas finalidades (minimização de dados); d) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; e) garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; f) garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados; g) utilização de medidas



técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; h) adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; i) impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; j) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nesse sentido, pelos princípios da minimização, da finalidade e da adequação do tratamento de dados, só poderão ser coletados os dados estritamente necessários ao fim para o qual foram coletados, bem como tais informações só poderão ser submetidas aos procedimentos que sejam adequados ao alcance dessa finalidade. Outrossim, os agentes de tratamento não poderão realizar procedimentos que visem a outro fim além do que fora informado ao titular dos dados.

Isso significa uma importante mudança de comportamento por parte de muitas organizações empresárias, as quais frequentemente coletam dados pessoais de maneira bastante extensiva, reunindo informações que vão muito além das realmente necessárias ao fornecimento de um produto ou serviço. A lógica de coletar e armazenar uma imensidão de dados que um dia poderão ou não vir a ser utilizados deve ceder à lógica da limitação da coleta aos dados realmente necessários à relação entre titular e agente de tratamento.

Ademais, de acordo com o princípio da não discriminação, os dados pessoais não poderão ser monetizados de maneira abusiva ou que leve a fins discriminatórios ilícitos, como, por exemplo, a venda de um mesmo produto ou serviço, no mesmo dia e horário, por preços diferentes a duas pessoas distintas motivada apenas pela análise de informações pessoais.

Buscando assegurar a realização desses princípios, a Lei Geral de Proteção de Dados Pessoais garante, ainda, uma série de direitos ao titular dos dados pessoais, a saber, a confirmação da existência de tratamento; o acesso aos dados; a correção de dados incompletos, inexatos ou desatualizados; a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; portabilidade dos dados a outro fornecedor de serviço ou produto; eliminação dos dados pessoais tratados com o consentimento do titular; informação das entidades públicas e



privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento; e revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses (arts. 18 e 20).

Dessarte, a referida Lei confirma que a titularidade de tais dados pertence à pessoa a quem as informações se referem, bem como atribui ao indivíduo maior controle sobre seus dados, permitindo que ele possa revogar seu consentimento, bem como pedir a eliminação de suas informações do banco de dados, por exemplo. As organizações empresárias que monetizam dados pessoais, por sua vez, deverão se adequar à LGPD, se não quiserem sofrer sanções administrativas, além de estarem sujeitas à responsabilidade civil.

Além disso, consagra um direito geral de informação, assegurando aos indivíduos o direito de tomarem conhecimento a respeito dos bancos de dados existentes, de quem é o responsável pelo tratamento de dados, qual o objetivo do tratamento, bem como quais são os destinatários dos dados em caso de transferência. Outrossim, a pessoa deve ser informada de quais são os seus direitos e quais as formas de exercê-los em cada fase do tratamento de dados pessoais.

Dessa forma, o agente de tratamento deverá permitir que os titulares dos dados tomem conhecimento da monetização de suas informações, da forma como ocorre tal prática, qual o fim de tal monetização, bem como se os dados pessoais monetizados são transferidos ou podem ser acessados por terceiros.

Ademais, uma vez que os dados pessoais são uma projeção da personalidade do indivíduo, a LGPD garante que este possa fazer as correções, complementações e supressões necessárias à exatidão de seus dados, permitindo uma representação mais fidedigna da realidade, o que também deve ser observado no tratamento que monetize tais informações.

Também o compartilhamento dos dados pessoais, gratuito ou oneroso, sofrerá restrições. A esse respeito, o artigo 7º, § 5º, da LGPD expressamente prevê que o controlador “que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento”.

Diante disso, o agente de tratamento que cede sua base de dados para terceiros deverá obter o consentimento do titular das informações pessoais para tanto, o qual deverá ser



informado acerca de quais dados serão compartilhados e para quais finalidades serão utilizados.

Importa dizer, ainda, que a atuação da Autoridade Nacional de Proteção de Dados também será fundamental no que diz respeito à monetização dos dados pessoais sensíveis, haja vista que o artigo 11, § 3º, da LGPD dispõe que a ANPD poderá regulamentar e até mesmo vedar a comunicação ou o uso compartilhado dessas informações entre controladores com objetivo de obter vantagem econômica.

Entretanto, no que atine aos dados pessoais sensíveis referentes à saúde, a Lei nº 13.709/2018 já proíbe a comunicação ou o uso compartilhado desses dados com o objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados ou a realização de transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo (art. 11, § 4º).

Outro ponto que levantará questionamentos é se a monetização de dados pessoais poderá ser feita com base na autorização da LGPD para que o tratamento de dados ocorra, independentemente do consentimento do titular, quando necessário para atender aos interesses legítimos do controlador ou de terceiro. A esse respeito, dispõe o artigo 10 da Lei Geral de Proteção de Dados Pessoais:

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

- I - apoio e promoção de atividades do controlador; e
- II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

A abertura dessa cláusula geral pode levar ao argumento de que a monetização de dados pessoais é interesse legítimo do controlador, uma vez que muitas organizações empresárias tem nesta atividade sua maior fonte de receita.

Entretanto, o legítimo interesse não pode ser utilizado para justificar todo e qualquer tratamento de dados pessoais. A própria lei traz os limites que devem ser observados, quais sejam, os direitos e liberdades fundamentais do titular dos dados, assim como as suas legítimas expectativas.





Nessa senda, a possibilidade de o interesse legítimo fundamentar ou não determinado procedimento demandará uma análise a partir de situações concretas, a qual deverá, além de realizar uma ponderação entre o interesse do controlador e os direitos do titular, observar a inexistência de abuso de direito, bem como o respeito aos princípios e valores do ordenamento jurídico e se o referido tratamento é realmente necessário e adequado, isto é, se não havia alternativas que fossem menos perigosas à privacidade do titular (BUCAR; VIOLA, 2019, p. 482).

Aqui, mais uma vez a Autoridade Nacional de Proteção de Dados terá um papel fundamental, haja vista que, dada a sua especialidade “a ela caberá definir qualitativamente os parâmetros do interesse legítimo, comungando-se o conhecimento técnico das formas de tratamento com sua respectiva juridicidade”, isto é, a Autoridade poderá fornecer importantes subsídios para a aplicação concreta da cláusula aberta do interesse legítimo (BUCAR; VIOLA, 2019, p. 475).

Por fim, a Lei Geral de Proteção de Dados Pessoais também dispõe que estas informações deverão ser eliminadas após o término de seu tratamento, autorizada a conservação para as seguintes finalidades: cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência à terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Isso posto, como regra, o agente de tratamento não poderá manter os dados pessoais em sua base para fins de monetização após o término do tratamento de dados, inclusive depois de o titular comunicá-lo do encerramento ou revogar o consentimento que forneceu para a manipulação de dados. Entretanto, se os dados forem anonimizados, o agente de tratamento poderá continuar a utilizá-los, o que demonstra a anonimização como uma importante ferramenta para que as organizações empresárias concretizem seus modelos de negócio.

Como se vê, a Lei Geral de Proteção de Dados Pessoais trouxe importantes diretrizes a serem seguidas pelas organizações que resolvam monetizar esses dados, o que pode gerar algumas dificuldades de adaptação para os entes que realizam esse tipo de atividade.

Quando o Regulamento Geral de Proteção de Dados da União Europeia – Regulamento este que é a fonte de inspiração da LGPD e que possui disposições semelhantes



à lei brasileira – entrou em vigor, por exemplo, foi possível verificar consequências para organizações sediadas em países fora do continente europeu, mas que atuavam naquele continente. Observou-se, inclusive, implicações em organizações brasileiras que atuavam com a monetização de dados pessoais, com muitos empresários deixando sua atuação na Europa, por dificuldades para adequação de sua atuação com a nova legislação europeia (FONSECA, 2018).

Uma alternativa que pode ser viável aos agentes monetizadores é anonimizar os dados pessoais. A anonimização consiste na remoção ou na ofuscação de toda a informação pessoal de uma base de dados, com o objetivo de impedir a identificação dos indivíduos. Aplicam-se técnicas que pretendem tornar impraticável, ou razoavelmente impossível, a reidentificação, inclusive pelo próprio técnico que realizou a operação inicial (PINHO, 2017, p. 29). De tal modo, essas técnicas retiram o vínculo entre o dado e o seu titular (DONEDA, 2019, p. 140). Em suma, considera-se anônimo aquele dado que seja “incapaz de revelar a identidade de uma pessoa” (BIONI, 2019, p. 70).

Isso porque a Lei Geral de Proteção de Dados, em seu artigo 12, estabelece que os dados anonimizados não serão considerados dados pessoais para os fins da Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Dessa forma, uma vez anonimizados, afasta-se a incidência da LGPD, de modo que o fornecimento do consentimento do titular ou a caracterização do interesse legítimo deixam de ser necessários à realização do tratamento de dados.

É claro, no entanto, que nem todos os procedimentos de monetização podem ser realizados se os dados estiverem anonimizados. Nesse caso, o agente de tratamento deverá observar todas as disposições previstas na LGPD no desenvolvimento do seu modelo de negócio, sob pena de sofrer severas sanções administrativas, como multa; bloqueio ou eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados; suspensão temporária do exercício da atividade de tratamento dos dados pessoais; proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados; entre outras.

## CONCLUSÃO







Como visto, na economia da informação, os dados pessoais tornam-se os mais valiosos ativos de grandes organizações empresárias, principalmente daquelas ligadas ao setor de tecnologia, como o *Google* e o *Facebook*. Nesse cenário, essas informações são monetizadas, isto é, os dados pessoais são submetidos a determinados tratamentos que os transformam em informações de valor, seja por serem utilizadas como um instrumento para facilitar transações seja por se tornarem o próprio objeto dessas transações.

Desse modo, determinada organização pode coletar e tratar os dados de seus clientes e, a partir dessas informações, personalizar o serviço prestado ou o produto vendido a esses mesmos clientes. Mas também essa mesma organização pode coletar e tratar os dados de seus clientes e repassá-los a um terceiro, mediante contraprestação, de modo que as informações tornam-se o próprio objeto da transação.

Essa prática que tem orientado muitos modelos de negócio não é ilícita. Entretanto, deve respeitar alguns limites jurídicos, especialmente aqueles decorrentes do direito à privacidade dos titulares dos dados.

Na prática, porém, quando ausente regulação específica sobre a proteção de dados pessoais, os empresários costumam coletar e tratar dados dos indivíduos sem nem mesmo informá-los disso. Além disso, não raramente os dados coletados são transferidos a terceiros sem a anuência do titular, que fica impossibilitado de exercer o controle sobre as suas informações.

Essas situações, bem como os grandes escândalos que envolveram o vazamento de milhões de dados de corporações como o *Facebook*, deixando uma imensidão de usuários expostos, têm feito crescer cada vez mais a preocupação com a privacidade das pessoas em meio aos modelos de negócio da economia informacional e levado à criação de legislação específica sobre a tutela dos dados pessoais, como a Lei nº 13.709/2018, no Brasil, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD), ainda em *vacatio legis*.

A referida Lei intenta regulamentar a coleta e o tratamento de dados pessoais no país, contudo, sem impossibilitar o desenvolvimento tecnológico e econômico. Nesse sentido, regulamenta a forma como o titular do direito aos dados pessoais poderá limitar seu exercício em favor de terceiros de maneira compatível com as características dos direitos da personalidade, isto é, mediante autorização do titular e de forma parcial e temporária. Dessa



forma, a monetização de dados pessoais continuará sendo legalmente possível, desde que ocorra em atenção à Lei nº 13.709/2018.

Assim, o primeiro ponto a ser observado pelos agentes que monetizam informações pessoais é que a LGPD somente autoriza o tratamento de dados mediante o fornecimento do consentimento pelo titular ou, independentemente deste, no caso de situações específicas expressamente previstas.

Portanto, a menos que o tratamento de dados pessoais esteja fundado em outra hipótese legal, o agente monetizador deverá obter o consentimento do titular, o qual deve ser livre, inequívoco e informado. Isso significa que a LGPD não autoriza que o silêncio seja considerado como manifestação da vontade. Além disso, o indivíduo deverá ser informado de quais dados estão sendo coletados, assim como a finalidade para a qual serão utilizados. Já no que diz respeito à liberdade do consentimento, como demonstrado, a atuação da Autoridade Nacional de Proteção de Dados será fundamental para estabelecer os parâmetros do que poderá ou não ser considerada manifestação livre.

Ademais, a Lei Geral de Proteção de Dados Pessoais prevê uma série de princípios que deverão ser observados quando da monetização de dados pessoais. Entre eles, destacam-se os princípios da minimização, da finalidade, da adequação do tratamento de dados e da não discriminação.

Nesse diapasão, só poderão ser coletados os dados estritamente necessários ao fim para o qual foram coletados, bem como tais informações só poderão ser submetidas aos procedimentos que sejam adequados ao alcance dessa finalidade. Ainda, os agentes de tratamento não poderão realizar procedimentos que visem a outro fim além do que fora informado ao titular dos dados, muito menos poderão ser monetizados de maneira abusiva ou com finalidade discriminatória.

Outrossim, para realizar o compartilhamento dos dados pessoais, seja ele gratuito ou oneroso, o agente de tratamento deverá obter o consentimento do titular das informações pessoais para tanto. Nesse ponto, mais uma vez será essencial a atuação da ANPD, uma vez que a Lei dispõe que a Autoridade poderá regulamentar e até vedar o uso compartilhado de dados sensíveis com objetivo de obter vantagem econômica, já trazendo previsão proibitiva dessa prática no que atine aos dados referentes à saúde.



Outro ponto que a Autoridade Nacional deverá enfrentar é se a monetização de dados pessoais poderá ser feita com fundamento no interesse legítimo do controlador, tendo em vista que muitas organizações empresárias tem nesta atividade sua maior fonte de receita. Contudo, essa possibilidade demandará análises a partir de situações concretas, cabendo à ANPD definir qualitativamente os parâmetros do interesse legítimo, fornecendo importantes subsídios para a aplicação concreta dessa cláusula aberta.

Isso posto, a Lei Geral de Proteção de Dados Pessoais atribui ao indivíduo maior controle sobre seus dados, bem como traz importantes diretrizes a serem seguidas pelas organizações que resolvam monetizar esses dados, o que poderá gerar algumas dificuldades de adaptação para os entes que realizam esse tipo de atividade. Nessa senda, a anonimização pode ser uma alternativa viável aos agentes monetizadores, uma vez que a LGPD não incide sobre o tratamento e manipulação de dados anonimizados, afastando-se a exigência do consentimento do titular, por exemplo.

Entretanto, não sendo possível a utilização de dados anonimizados, as organizações empresárias que monetizam dados pessoais deverão se adequar à LGPD, se não quiserem sofrer sanções administrativas, além de estarem sujeitas à responsabilização civil.

## REFERÊNCIAS

ADJEI, Joseph K. Monetization of Personal Identity Information: Technological and Regulatory Framework. **IEEE Computer Society Washington**, Washington DC/EUA, 14 dez. 2015. Disponível em: [https://www.researchgate.net/profile/Joseph\\_Adjei3/publication/325142873\\_Monetization\\_of\\_personal\\_digital\\_identity\\_information\\_Technological\\_and\\_regulatory\\_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-information-Technological-and-regulatory-framework.pdf](https://www.researchgate.net/profile/Joseph_Adjei3/publication/325142873_Monetization_of_personal_digital_identity_information_Technological_and_regulatory_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-information-Technological-and-regulatory-framework.pdf). Acesso em: 02 abr. 2020.

BIONI, Bruno Ricardo. **Proteção dos dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019.

BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por “legítimo interesse do controlador”: primeiras questões e apontamentos. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Orgs.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thompson Reuters Brasil, 2019.

CARVALHO, Victor M. B. de; GUIMARÃES, Patrícia B. V.; OLIVEIRA, Adriana C. Monetização de dados pessoais na internet: competência regulatória a partir do Decreto nº



8.771/2016. **Revista Estudos Institucionais**, Rio de Janeiro, v. 4, n. 1, 2018. Disponível em: <https://estudosinstitucionais.com/REI/article/view/215>. Acesso em: 02 abr. 2020.

CARVALHO, Victor M.B. de. **O Direito Fundamental à Privacidade ante a Monetização de Dados Pessoais na Internet: apontamentos legais para uma perspectiva regulatória**. 2018. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: [http://bdtd.ibict.br/vufind/Record/UFRN\\_9ee764a6de69a62f84e93f1356e90adb](http://bdtd.ibict.br/vufind/Record/UFRN_9ee764a6de69a62f84e93f1356e90adb). Acesso em: 02 abr. 2020.

CASTELLS, Manuel. *A Sociedade em Rede: A era da informação: economia, sociedade e cultura*. Vol. 1. São Paulo: Paz e Terra, 1999.

COHEN, Max E. Alguns aspectos do uso da informação na economia da informação. **Ciência da Informação**, v. 31, n. 3, 2002. Disponível em: [http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci\\_abstract&tlng=pt](http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt). Acesso em: 02 abr. 2020.

D'SOUZA, Chris; WILLIAMS, David. The Digital Economy. **Bank of Canada Review**, 2017. Disponível em: <https://www.bankofcanada.ca/wp-content/uploads/2017/05/boc-review-spring17-dsouza.pdf>. Acesso em: 02 abr. 2020.

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.

FONSECA, Mariana. GDPR: o que muda nas startups brasileiras com a nova lei de dados. **Exame**, 04 jun. 2018. Disponível em: <https://exame.abril.com.br/pme/gdpf-nova-lei-europeia-de-dados-pessoais-ja-afeta-startups-brasileiras/>. Acesso em: 02 abr. 2020.

GOOGLE. **Ajuda do Conta do Google – Gerenciar o Histórico de localização**. 2019a. Disponível em: <https://support.google.com/accounts/answer/3118687?hl=pt>. Acesso em: 02 abr. 2020.

GOOGLE. **Política de Privacidade**. 2019b. Disponível em: <https://policies.google.com/privacy?hl=pt-BR>. Acesso em: 02 abr. 2020.

GRUPO DE TRABALHO do Artigo 29.º para a Proteção de Dados. **Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/79**. 28 nov. 2017. Disponível em: [https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1\\_PT.pdf](https://www.cnpd.pt/home/rgpd/docs/wp259rev0.1_PT.pdf). Acesso em: 15 abr. 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor – linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

NAKASHIMA, Ryan. AP Exclusive: Google tracks your movements, like it or not. **AP News**, 13 ago. 2018. Disponível em: <https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb>. Acesso em: 02 abr. 2020.





O ESTADO DE SÃO PAULO. **Facebook e Google devem perder US\$ 44 bi em receitas por causa da pandemia.** 25 mar. 2020. Disponível em: <https://link.estadao.com.br/noticias/empresas,facebook-e-google-devem-perder-us-44-bi-em-receita-por-causa-da-pandemia,70003247727>. Acesso em: 15 abr. 2020.

PEIXOTO, Erick L. C; EHRHARDT JÚNIOR, Marcos. Breves Notas sobre a Ressignificação da Privacidade. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 16, p. 35-56, jan./jun. 2018. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230>. Acesso em: 12 jun. 2019.

PINHO, Frederico A. S. O. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados.** 2017. Dissertação (Mestrado em Segurança Informática), Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto. Disponível em: [https://cracs.fc.up.pt/sites/default/files/MSI\\_Dissertacao\\_FINAL.pdf](https://cracs.fc.up.pt/sites/default/files/MSI_Dissertacao_FINAL.pdf). Acesso em: 02 abr. 2020, p. 29.

ROCHFELD, Judith. Como qualificar os dados pessoais? Uma perspectiva teórica e normativa da União Europeia em face dos gigantes da Internet. **Revista de Direito, Estado e Comunicações**, Brasília, v. 10, n. 1, maio 2018. Disponível em: [http://www.mpsp.mp.br/portal/page/portal/documentacao\\_e\\_divulgacao/doc\\_biblioteca/bibli\\_servicos\\_produtos/bibli\\_boletim/bibli\\_bol\\_2006/Rev-Dir-Est-Telecom\\_v.10\\_n.01.04.pdf](http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Rev-Dir-Est-Telecom_v.10_n.01.04.pdf). Acesso em: 02 abr. 2020.

RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje.** Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SANTINO, Renato. Google recebeu mais de US\$ 15 bilhões com anúncios do YouTube em 2019. **Olhar Digital**, 03 fev. 2020. Disponível em: <https://olhardigital.com.br/noticia/google-recebeu-mais-de-us-15-bilhoes-com-anuncios-do-youtube-em-2019/96248>. Acesso em: 15 abr. 2020.

SCHREIBER, Anderson. **Direitos da Personalidade.** 3. ed. São Paulo: Atlas, 2014.

TODD, Steve. O valor dos dados em um mundo impulsionado por informações. **CANALTECH**, 23 out. 2015. Disponível em: <https://canaltech.com.br/big-data/o-valor-dos-dados-em-um-mundo-impulsionado-por-informacoes-51425/>. Acesso em: 02 abr. 2020.

TSUKAYAMA, Hayley. Don't want Google tracking you? You have almost no choice, according to a study. **The Washington Post**, 21 ago. 2018. Disponível em: [https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm\\_term=.a644e5215606](https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm_term=.a644e5215606). Acesso em: 02 abr. 2020.

UNIÃO EUROPEIA. **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados e que revoga a



Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados. Disponível em: <https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf>. Acesso em: 02 abr. 2020.

VITAL, Antonio. Proteção de dados: informações pessoais movimentam nova economia digital mundial – Bloco 4. **Rádio Câmara, Câmara dos Deputados**, Brasília, 05 mar. 2018. Disponível em: <https://www2.camara.leg.br/camaranoticias/radio/materias/REPORTAGEM-ESPECIAL/554146-PROTECAO-DE-DADOS-INFORMACOES-PESSOAIS-MOVIMENTAM-NOVA-ECONOMIA-DIGITAL-MUNDIAL-BLOCO-4.html>. Acesso em: 02 abr. 2020.

YAMAGATA, Nicolas. Monetizando você e seus dados com a função de inteligência. **Intelligence Hub**, 05 nov. 2017. Disponível em: <http://www.intelligencehub.com.br/monetizando-voce-e-seus-dados-com-funcao-de-inteligencia/>. Acesso em: 02 abr. 2020.

