AS NOÇÕES DE *DATA DRIVEN BUSINESS* E A CRESCENTE TUTELA JURÍDICA DE DADOS PESSOAIS NO BRASIL

THE CONCEPT OF DATA DRIVEN BUSINESS AND THE INCREASING LEGAL PROTECTION OF PERSONAL DATA IN BRAZIL

Rafael Sgoda Tomazeti[1]

Recebido/Received: 17.03.2023/Mar 17th, 2023
Aprovado/Approved: 03.04.2023/Apr 3rd, 2023

RESUMO: Este artigo analisa como a crescente tutela jurídica de dados pessoais impacta modelos de negócios orientados por dados (data driven business), no contexto de uma sociedade informacional. Apresentando a importância dos dados pessoais na economia atual e o histórico de normas de privacidade e proteção de dados pessoais no cenário nacional, o trabalho também lista sugestões para compatibilizar as leis vigentes com modelos de negócios que utilizam dados como matéria-prima ou linha mestra. Utilizando métodos de pesquisa quantitativos e qualitativos, como pesquisas sobre uso de dados e levantamento legislativo e doutrinário, conclui-se que é possível proteger os dados pessoais sem impedir a inovação e o desenvolvimento econômico, tendo em vista que o legislador adotou normas flexíveis com este fim.
PALAVRAS-CHAVE: dados pessoais; *data driven business*; inovação; sociedade informacional; informação.

ABSTRACT: This article analyzes how the increasing legal protection of personal data impacts data-driven business models in the context of an informational society. Presenting the importance of personal data in the current economy and the history of privacy and personal data protection regulations in the Brazilian scenario, the work also lists suggestions for reconciling existing laws with business models that use data as raw material or guiding principle. Using quantitative and qualitative research methods, such as surveys on data usage and legislative and doctrinal surveys, it is concluded that it is possible to protect personal data without impeding innovation and economic development, considering that the Brazilian legislator has adopted flexible rules for this purpose.
KEYWORDS: personal data; data-driven business; innovation; informational society; information.

[1] Mestrando em Direito das Relações Sociais pelo Programa de Pós-Graduação em Direito da Universidade Federal do Paraná (UFPR). Especialista em Compliance e Integridade Corporativa pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas) e em Direito Empresarial pela Faculdade Legale. Graduado em Direito pelo UniBrasil - Centro Universitário Autônomo do Brasil. Advogado. Currículo Lattes: http://lattes.cnpq.br/5139889281912020. E-mail: rafael.tomazeti@outlook.com

INTRODUÇÃO

De cada vez maior reconhecimento, a expressão “sociedade informacional” (ou, ainda, “sociedade da informação” ou “sociedade pós-industrial”[1]) é comumente ligada ao sociólogo Daniel Bell (1974, p. 148-149), que, já na década de 70, reconhecia um novo fenômeno social, defendendo que os serviços baseados no conhecimento ganhariam papel de destaque na economia, considerando que as atividades industriais já se encontravam em declínio.

Além da superação do emprego industrial pelo setor de serviços nos Estados Unidos, Bell defendia essa nova realidade pós-industrial porque as fontes de inovação dependeriam cada vez mais do conhecimento – o qual seria um importante aliado ao desenvolvimento e às decisões políticas (BELL, 1974, p. 199).

Atualmente, não restam dúvidas da importância do conhecimento para a nova economia.

Exemplificativamente, uma forma simples de visualizar o valor do conhecimento e/ou da informação é a mudança do foco do *marketing* na nova realidade social. Como aponta Bauman (2014, p. 85), “a grande evolução (...) no progresso da sociedade consumista foi a passagem da satisfação das necessidades (...) para sua criação (...), por meio de tentação, sedução e estímulo do desejo assim despertado”.

Com efeito, os dados se tornaram de grande valia para compreender comportamentos, atitudes, interesses e expectativas, permitindo a criação de estratégias voltadas a melhor atender públicos-alvo, criar novas necessidades e desejos, antever cenários e oferecer novas soluções.

Esta nova realidade, proporcionada pelo avanço da ciência e da tecnologia, permitiu a criação de negócios que têm como matéria-prima e/ou fio condutor o tratamento de dados – o que ficou conhecido como “*data driven business*” (“negócio

[1] No presente trabalho e conforme as lições de Manuel Castells, utiliza-se a expressão “sociedade informacional” para referenciar o fenômeno, por compreendê-la como mais adequada. Por oportuno, registre-se que para o professor “sociedade da informação” destacaria o papel da informação na sociedade – o que, no entanto, transmitiria uma ideia de comunicação de conhecimento, que foi importante em todas as sociedades, inclusive na Europa medieval. Por sua vez, “o termo informacional indica o atributo de uma forma específica de organização social em que a geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico” (CASTELLS, 2021, p. 84).

orientado a dados", em tradução livre), cujo modelo de gestão parte da análise de dados para a tomada de decisões.

Em paralelo, no entanto, o uso indiscriminado de informações, principalmente de pessoas naturais, trouxe novas preocupações, tornando forçoso o aprimoramento e reforço da tutela jurídica de tais ativos, inclusive no Brasil.

Destarte, este trabalho dedica-se a analisar eventuais interesses e desafios envolvidos no presente cenário. Para tanto, a pesquisa adota como principal marco teórico a teoria da sociedade em rede de Manuel Castells (2021, p. 81), caracterizada por ser uma "teoria transcultural exploratória da economia e da sociedade na Era da Informação", que compreende que a fonte de produtividade está nas tecnologias de "geração de conhecimentos, de processamento das informações e de comunicação de símbolos" (CASTELLS, 2021, p. 74).

Metodologicamente, utilizam-se métodos quantitativos, consubstanciados, por exemplo, em pesquisas, de modo a compreender de forma pragmática a importância da utilização de dados no contexto atual, e métodos qualitativos, como levantamento bibliográfico e dogmático, inclusive legislativo e jurisprudencial, de modo a cotejar a atual tutela jurídica de dados pessoais e as noções de *data driven business*.

Finalmente, cabe pontuar que este trabalho foi dividido em quatro partes principais. Na primeira, se analisará o conceito de *data driven business* e sua inserção no contexto da sociedade informacional; na segunda, se destacará a preocupação no uso de dados pessoais que impulsionou mudanças na tutela jurídica de tais ativos; na terceira, se apresentará o panorama da crescente proteção de dados pessoais no ordenamento jurídico brasileiro; e, na última, serão pontuadas pontenciais conflitos entre o uso de dados pessoais e a tutela legal, de modo a identificar desafios e cuidados a serem observados no contexto atual.

1 O CONCEITO DE *DATA DRIVEN BUSINESS* E SUA RELEVÂNCIA NA SOCIEDADE INFORMACIONAL

As transformações sociais proporcionadas pela dita sociedade informacional exigiram e exigem também a evolução do ordenamento jurídico. Desde o direito romano, fixou-se o brocardo *ex factor oritur jus* (o Direito nasce do fato), denotando sua dependência dos quereres sociais, do local e da época em que se situa (NADER, 2014, p. 149-150).

Assim, compreender o contexto social é fundamental para entender, posteriormente, a crescente tutela jurídica de dados pessoais e, consequentemente, garantir uma melhor aplicação do direito.

Como explica o professor Wolfgang Hoffmann-Riem (2021, p. 1), desde o final do último milênio, a sociedade vivencia uma terceira "convulsão tecnológica" que causa e causará grandes modificações no cotidiano. Assim como as duas primeiras "convulsões" ou "inovações tecnológicas 'disruptivas'", quais sejam, a invenção de impressão tipográfica e a industrialização, o fenômeno da "digitalização" tem transformado, digitalmente, várias searas da vida, como a cultura e a política.

Essa "digitalização" compreende uma série de inovações, tecnologias e técnicas, que, dentre outras possibilidades, passou a permitir que uma grande quantidade de dados fosse tratada com um propósito específico de gerar algum tipo conhecimento a ser utilizado beneficamente.

Convencionou-se chamar esse alto desempenho para tratamento de dados de "*big data*" e as lições doutrinárias auxiliam na sua compreensão:

> O termo *Big Data* refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinação, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos. Cinco características são frequentemente utilizadas para identificar *Big Data*: Os cinco "Vs" [sic]. As possibilidades de acesso a enormes quantidades de dados digitais (*High Volume*), de diferentes tipos e qualidade, assim como diferentes formas de coleta, armazenamento e acesso (*High Variety*), e a alta velocidade do seu processamento (*High Velocity*). O uso da inteligência artificial em particular torna possível novas e altamente eficientes formas de processamento de dados, bem como verificação de sua consistência e garantia de qualidade (*Veracity*). Além disso, os *Big Data* são objeto e base de novos modelos de negócios e de possibilidades para diversas atividades de valor agregado (*Value*) (grifos no original) (HOFFMANN-RIEM, 2021, p. 16-17).

Destarte, com o uso de *big data* (que realiza o processamento de elevadas quantidades de dados em altíssima velocidade) é possível descobrir "padrões", isto é, verificar "a recorrência de um evento que permite prever que eles se repetirão no futuro" (BIONI, 2019, p. 58).

Em outros termos, o *big data* permite o tratamento – aqui entendido como qualquer operação realizada com dados, como a coleta, o processamento, a

comparação, avaliação, entre outras – gerando informação e, consequentemente, conhecimento[1] – de inegável valia na sociedade atual.

Com efeito, a facilidade de coleta e processamento de dados tornou a informação o ativo estruturante da economia contemporânea. Se na sociedade agrícola o núcleo basilar de organização da sociedade eram as terras; na sociedade industrial, os maquinários; e, na sociedade pós-industrial, os serviços, agora vivencia-se uma sociedade informacional (BIONI, 2019, p. 33).

Por óbvio, não se quer afirmar que a informação era desprovida de valor anteriormente, mas as tecnologias disponíveis e a "digitalização" de quase todo tipo de dado, permite que mais dados estejam disponíveis e possam ser tratados em alta escala e velocidade, permitindo a geração de informações (e conhecimento) com níveis de sofisticação, precisão e atualização anteriormente inatingíveis (MIELE; SHOCKLEY, 2013).

É possível, inclusive, afirmar que o uso da informação se tornou tão importante para a sociedade contemporânea que pode ser entendida como elemento vital para a perenidade dos negócios.

Pesquisa realizada em 2012 pelo IBM (*Institute for Business Value*) em colaboração com a *Saïd Business School* da Universidade de Oxford apontou que o *big data* não é utilizado apenas por grandes corporações, sendo que, à época do levantamento, empresas de médio porte também já estavam compreendendo a importância dessa tendência ou a estavam utilizando de alguma forma.

Com a participação de 1.144 (um mil, cento e quarenta e quatro) organizações e profissionais de tecnologia da informação em 95 (noventa e cinco) países, apenas 18% (dezoito por cento) de grandes corporações ainda não haviam iniciado nenhuma atividade com o uso de *big data*. Em empresas de médio porte, esse percentual chegava a 28% (vinte e oito por cento) (MIELE; SHOCKLEY, 2013).

A maioria, portanto, afirmou já estar compreendendo a tecnologia e elaborando um projeto-piloto ou mesmo implementando-a ou utilizando-a.

Ainda segundo o levantamento, quase metade dos participantes (quarenta e seis por cento das empresas de médio porte e quarenta e oito por cento das empresas de grande porte) afirmou que objetiva utilizar as técnicas de *big data* para

[1] Sem prejuízo de posições doutrinárias divergentes, a "informação" é compreendida como o agrupamento de dados para construir um sentido semântico a partir deles e, após a sua compreensão e interpretação, se torna "conhecimento" (SEMIDÃO, 2014).

melhor compreender seu público (suas preferências e seus comportamentos, para descobrir novas maneiras de envolver/engajar consumidores atuais e em potencial) (MIELE; SHOCKLEY, 2013).

Certamente, compreender o comportamento e as expectativas do público-alvo pode ser um importante aliado na sustentabilidade do negócio e, como consequência lógica, esse conhecimento pode auxiliar na identificação de demandas que geram a criação de novos negócios[1].

Não por outra razão, em outra pesquisa realizada pelo IBM (*Institute for Business Value*) com 1.004 (um mil e quatro) executivos de alto escalação[2], verificou-se que, em organizações com alto desempenho, o uso de *big data* é 23% (vinte e três por cento) mais provável e o uso de análises é 79% (setenta e nove por cento) mais provável para identificar oportunidades inovadoras (IKEDA; MARSHALL; MAJUMDAR, 2016).

Em outras palavras, deter e tratar informações se torna um ferramental estratégico para o sucesso empresarial.

Nesta conjuntura, forçoso concluir que os dados passaram a ter papel relevante na condução dos negócios – o que ficou conhecido como "*data driven business*", ou seja, "negócios orientados por dados" em tradução livre.

É desse reconhecido valor aos dados que atualmente existem modelos de negócios baseados exclusivamente ou, quando menos, primordialmente no tratamento de dados – os quais recebem, pela doutrina, o nome "*data-driven business models*" ou, na sigla, DDBM (HARTMANN, *et. al.*, 2016, p. 1382-1406). É o caso, por exemplo, de serviços de busca na internet, comércios eletrônicos e mídias sociais (BÖHMECKE-SCHWAFERT; NIEBEL, 2018, p. 2).

[1] Ter informações e gerar conhecimento sobre seu público não apenas pode auxiliar na identificação da oferta e demanda de produtos ou serviços, mas também na avaliação de riscos – outro ferramental que auxilia na perenidade dos negócios. Na era da "digitalização" também se criou uma tendência chamada "KYC", "*Know Your Customer"* ou, ainda "*Know Your Client*" que, em tradução literal, significa "Conheça seu Cliente/Consumidor". A expressão visa definir a prática de avaliação de uma pessoa (consumidor/cliente) para identificar riscos de uma contratação ou parceria, a partir de suas características. Em respeito ao objeto deste estudo, o tema não será analisado em profundidade, mas a técnica é muito conhecida no sistema financeiro, sendo obrigatória em alguns casos, mormente para evitar práticas de lavagem de dinheiro.

[2] Os profissionais que participaram da pesquisa encontravam-se em cargos denominados "*C-Level*" ou "*C-Suite*". A expressão visa designar cargos de chefe (*chief*), como CEO (*Chief Executive Officer*), COO (*Chief Operating Officer*), entre outros.

2 A PREOCUPAÇÃO NO USO DE DADOS PESSOAIS

Como alhures exposto, os dados ganharam papel de destaque na sociedade e economia atuais e, indiscutivelmente, podem ser tratados de incontáveis formas para produzir informação para também incontáveis finalidades. Contudo, para que os dados sejam tratados e se tornem informação (e, posteriormente, conhecimento), certamente é necessário que estejam disponíveis, ou seja, é preciso que, de alguma forma, sejam coletados, capturados ou produzidos para que posteriormente sejam avaliados, comparados e tratados em geral.

O avanço tecnológico (incluído o uso de *big data*), combinado com a digitalização de praticamente todo tipo de dado, também facilitou a disponibilidade desses dados. Isto é, o avanço tecnológico não apenas permitiu que um grande volume de dados seja avaliado, classificado, comparado em uma alta velocidade, mas também auxiliou o descobrimento desses dados – afinal, "o uso de técnicas digitais requer dados em forma digitalizada" (HOFFMANN-RIEM, 2021, p. 13).

É justamente em razão dessa digitalização praticamente universal de tudo e todos que a vigilância passa a ser basilar na economia contemporânea (BIONI, 2019, p. 64).

Se os dados devem estar disponíveis para que sejam tratados e sejam transformados em informação, é preciso encontrar formas de disponibilizá-los e a adoção de métodos de vigilância (nem sempre claros ou explícitos) se vê cada vez mais presente.

Importante pontuar, neste momento, que a natureza desses dados pode ser de diferentes ordens. Eles podem se referir a uma pessoa natural, a uma pessoa jurídica, a um produto, a um serviço, entre outros.

Quando se referem a uma pessoa natural, convencionou-se denomina-los de "dados pessoais". Neste contexto, o art. 5º, inc. I, da Lei Geral de Proteção de Dados Pessoais (ou, simplesmente, "LGPD") (Lei nº 13.709/18), melhor abordada a seguir, conceitua "dado pessoal" como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).

Veja-se, portanto, que não é todo e qualquer tipo de dado que é tutelado pelo mencionado diploma legal, mas apenas quando relacionado a uma pessoa natural que seja "identificada ou identificável". Dados de pessoas jurídicas ou de pessoas

que não possam ser identificadas[1], por exemplo, encontram-se fora do seu âmbito de aplicação.

Essa distinção é de importante valia, porquanto as recentes legislações que protegem dados pessoais decorrem justamente da invasão desse modelo econômico pautado na vigilância na esfera individual da pessoa natural (e no seu direito à privacidade). As consequências desse modelo vigilante para uma pessoa jurídica certamente serão diferentes daquelas sofridas por uma pessoa natural.[2]

A proteção dos dados pessoais não é uma preocupação exclusivamente brasileira. A bem da verdade, sem prejuízos de previsões pontuais e mais simples, o microssistema jurídico pátrio de proteção de dados pessoais aprimorado pela Lei Geral de Proteção de Dados Pessoais, promulgada em 2018 e que entrou em vigor na sua maior parte em 2020, chegou com certo atraso, em comparação a outros países, que já vinham há décadas discutindo a temática e editando regulamentos com maior robustez.

Os ensinamentos da professora Patricia Peck Pinheiro corroboram a informação de que a tutela jurídica de dados pessoais decorreu, justamente, da forma de organização da sociedade informacional. Vejamos:

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização (PINHEIRO, 2020, p. 12).

É importante pontuar que mesmo em negócios “B2B” (*Business-to-business*), em que a relação comercial se desenvolve entre organizações/pessoas jurídicas, os dados pessoais podem ser relevantes e valiosos, porquanto, por trás dessa ficção jurídica, existem pessoas naturais que, em última instância, são os tomadores de decisão.

---

[1] Nesta conjuntura, os arts. 5º, inc. III e 12, ambos da LGPD, informam que os “dados anonimizados” (assim considerados como aqueles em que o titular não possa ser identificado), em regra, não serão considerados como “dados pessoais” para o disposto na 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.

[2] Registre-se, por oportuno, que os dados de pessoas jurídicas também são tutelados pelo direito, mas através de regramentos diferentes. As normas previstas na LGPD são aplicáveis aos dados pessoais, mas os dados de pessoas jurídicas encontram proteção direta ou indiretamente na Lei Antitruste (Lei nº 12.529/11), na Lei de Propriedade Industrial (Lei nº 9.279/96), no Código Penal (Decreto-Lei nº 2.848/40) e na Consolidação das Leis do Trabalho (Decreto-Lei nº 5.452/43), entre outras.

Assim, o alto valor conferido aos dados na sociedade informacional, combinado com o fenômeno da digitalização, criou um “varejo dos dados pessoais”, onde as informações são matéria-prima para a geração de riqueza (BIONI, 2019, p. 64). Quanto maior a disponibilidade do dado pessoal, ou seja, quanto mais informações estão disponíveis, maior a vigilância exercida e mais eficiente o tratamento tende a ser para a finalidade pretendida.

Em que pese o inegável valor dos dados pessoais, não se pode ignorar possíveis interesses contrapostos no seu tratamento.

Como visto alhures, o direito é fruto do contexto e das demandas sociais e, com o avanço tecnológico e o modelo de vigilância, passou a ser instrumento para equilibrar “interesse comercial, privacidade, responsabilidade e anonimato” (PINHEIRO, 2013, p. 52). Com efeito, é razoável compreender que uma coleta desarrazoada ou um tratamento ilimitado de informações sobre determinada pessoa pode ser considerado como abusivo, capaz de ferir a sua privacidade.

Um dos casos mais emblemáticos para compreender a necessidade de se estabelecer limites ao tratamento de dados pessoais é o episódio que ficou conhecido como “Facebook-Cambridge Analytica”.

A Cambridge Analytica, organização privada de análise de dados, que trabalhou na eleição presidencial norte-americana de 2016 para a equipe de Donald Trump e também na campanha do Brexit, coletou e tratou um volume gigantesco de dados pessoais a partir de perfis de usuários do Facebook (no primeiro caso, por exemplo, de eleitores norte-americanos) e criou um poderoso *software* para prever e influenciar escolhas nas urnas eleitorais (THE GUARDIAN, 2018).

Dentre outras ações da Cambridge Analytica, a organização patrocinava conteúdos direcionados, que indicavam, por exemplo, os prós e contras de cada um dos candidatos, de acordo com as preferências do usuário destinatário da propaganda. Em termos práticos, a Cambridge Analytica criava e direcionada os conteúdos, considerando os dados previamente coletados do usuário, para influenciar suas decisões nos processos eleitorais.

A partir do momento que se confere valor aos dados pessoais, eles passam ser uma moeda de pagamento – como é o caso do próprio Facebook, que coleta consentimento de seus usuários para poder utilizá-los diretamente ou através de parceiros de negócios.

Não por outra razão, atualmente, existem modelos de negócios em que o pagamento é realizado exclusivamente a partir da oferta de dados pessoais – o que, sopesando com o direito à privacidade e à proteção de dados pessoais (que, no Brasil, são assegurados constitucionalmente), acaba por gerar debates sobre o estabelecimento de eventuais limites e qual o papel a ser desempenhado pelos instrumentos jurídicos ou, melhor, pelo Estado (PINHEIRO, 2013, p. 53).

A doutrina exemplifica esse embate:

> O que pode ser feito com esses dados [pessoais]? As empresas têm alterado suas políticas de privacidade para garantir maior propriedade dos dados para elas. Afinal, essa é a moeda de troca do uso do serviço. Mas como medir se é justo e proporcional? Será que a informação no seu perfil da rede social de que você tem como *hobby* jogar tênis permite que uma empresa use-a para abordá-lo? Seja para oferecer uma raquete de brinde ou vender uma assinatura de clube? (PINHEIRO, 2013, p. 53).

Enfrentando esses novos desafios causados pela sociedade atual, os Estados têm atualizado seus ordenamentos jurídicos, buscando de alguma forma sopesar os interesses econômico e pessoal envolvidos – e no Brasil não seria diferente.

3 A (CRESCENTE) TUTELA JURÍDICA DE DADOS PESSOAIS NO BRASIL

Didaticamente, a doutrina convencionou separar as normas jurídicas protetivas de dados pessoais em quatro “gerações” (BIONI, 2019, p. 174 e ss.).

A primeira geração das leis de proteção de dados era caracterizada pela necessidade de concessão de autorizações pelo Poder Público para a criação de bancos de dados pessoais, os quais também eram controlados pelas autoridades legais. Em alguns casos, apenas ao Estado era assegurada a possibilidade de controlar esses bancos.

Em seguida, reconhecendo sua incapacidade para administrar todos os bancos de dados, o Poder Público passou a editar leis que transferiam aos titulares dos dados a responsabilização pelo fornecimento ou não de tais informações, como se fosse uma “liberdade negativa” do indivíduo.

A terceira geração das leis de proteção de dados pessoais, por sua vez, era caracterizada pela autodeterminação informativa, com normas jurídicas que asseguravam ao titular o direito à informação e a consentir com o seu uso, trazendo mecanismos de defesa e passando a regular também outras operações de tratamento de dados, que não apenas a coleta através do consentimento. A

evolução legislativa se deu em razão da crescente importância dos dados pessoais, que passaram a se tornar cada vez mais necessários para o convívio social.

Finalmente, a quarta e atual geração destina-se a categorizar as legislações que passam a prever ainda maiores direitos ao titular dos dados e estabelecer mecanismos de segurança e controle de dados pessoais, garantindo transparência nas operações de tratamento de dados realizadas e maior proteção em determinados segmentos ou atividades. Exemplificativamente, as leis passaram a trazer categorias de dados pessoais com maior proteção e criar autoridades governamentais responsáveis por zelar pelo seu cumprimento.

A Lei Geral de Proteção de Dados Pessoais é a primeira legislação pátria desta quarta geração e também a primeira com caráter mais geral.

Até sua aprovação, o ordenamento jurídico brasileiro apresentava uma "colcha de retalhos", com algumas normas jurídicas setoriais que tratavam da proteção de dados pessoais (BIONI, 2019, p. 133).

Neste ínterim, pode-se destacar o artigo 43 do Código de Defesa do Consumidor – CDC (Lei nº 8.078/90) que, desde sua edição, disciplina os "bancos de dados e cadastros de consumidores" (BRASIL, 1990). O dispositivo traz algumas normas que afirmam, indene de dúvidas, que a titularidade das informações pessoais pertence à pessoa natural (no caso específico, ao consumidor). Exemplificativamente, o artigo prevê a obrigação de comunicação prévia e por escrito do consumidor sobre a abertura de cadastro, quando não solicitada por ele; o direito de correção de dados pessoais a pedido do consumidor; entre outros.

Mais tarde, em 2011, a Lei do Cadastro Positivo (Lei nº 12.414/11) estabeleceu regras para a formação de bancos de dados com informações de adimplemento, seja de pessoas naturais, seja de pessoas jurídicas (BRASIL, 2011). No seu artigo 5º, o diploma trouxe uma série de direitos do cadastrado, que demonstram uma preocupação em manter o controle dos dados com seu titular. Por exemplo, a legislação prevê o direito de obter o cancelamento ou reabertura de cadastro, quando solicitada; o direito de acesso às informações existentes no cadastro; e, o direito de conhecer os principais critérios e elementos considerados na classificação eventual realizada pelo banco de dados.

Em 2013, o Decreto do Comércio Eletrônico (Decreto nº 7.962/13) também fez menção aos dados pessoais ao estabelecer como obrigação do fornecedor a

utilização de “mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor” (art. 4º, inc. VII) (BRASIL, 2013).

Nova tutela jurídica de dados pessoais ficou sob o encargo do Marco Civil da Internet – MCI (Lei nº 12.965/14). De acordo com a legislação, a proteção dos dados pessoais é um dos princípios que disciplina o uso da internet no Brasil (art. 3º, inc. III) (BRASIL, 2014). Mais especificamente, o art. 7º, inc. VII à X, do MCI, apresenta alguns direitos relacionados aos dados pessoais, como o direito de não fornecimento a terceiros de tais informações, salvo mediante consentimento ou autorização legal; o direito de acesso a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados; a exclusão dos dados ao término da relação com a aplicação da internet; entre outros.

Ao longo do diploma legal, também são encontrados outros dispositivos que demonstração preocupação com o uso de dados pessoais e a privacidade na internet.

Veja-se, portanto, que apesar do legislador demonstrar certa preocupação com o tratamento de dados pessoais, as normas jurídicas estabelecidas tinham seu campo de atuação limitado a determinados setores ou tipos de relações jurídicas (no CDC, protegem-se os dados de consumidores; na Lei do Cadastro Positivo, as informações de crédito e adimplemento; e, no MCI, os dados presentes na rede mundial de computadores).

Foi apenas com a Lei Geral de Proteção de Dados Pessoais – LGPD que o país passou a contar com uma legislação ampla, destinada a abarcar uma infinidade de atividades de tratamento de dados pessoais. Ao contrário das legislações anteriores, a LGPD, em regra geral, tutela todos os dados pessoais, de modo que a sua inaplicabilidade tem caráter excepcional.[1]

A LGPD é fruto de debates que remontam há pelo menos uma década (BIONI, 2019, p. 187) após o reconhecimento da necessidade de proteção de tais ativos em razão do rápido desenvolvimento e expansão da tecnologia no mundo (PINHEIRO, 2020, p. 57), como alhures exposto.

[1] O art. 4º da LGPD elenca as atividades de tratamento que não são sujeitas à sua aplicação, dentre as quais se incluem o tratamento realizado por pessoa natural pra fins exclusivamente particulares e não econômicos e para fins exclusivamente jornalísticos e artísticos. Por seu turno, o art. 3º da legislação destaca o caráter extraterritorial da legislação. Em uma interpretação *a contrario sensu*, é possível identificar, por exemplo, que atividades que não sejam realizadas no território nacional com dados que não tenham origem no Brasil, são excluídos de sua aplicação.

Para a professora Pinheiro (2020, p. 57-58), “a LGPD advém da evolução e expansão dos direitos humanos e resulta da atualização/adaptação de documentos internacionais de proteção aos direitos humanos”.

Fortemente influenciada pela GDPR (*General Data Protection Regulation*) (Regulation EU 2016/679) (UNIÃO EUROPEIA, 2016), legislação que trata da proteção de dados pessoais na União Europeia, a LGPD apresenta, dentre outros pontos, o conceito de “dado pessoal”; os princípios que regem a matéria; os requisitos para que o tratamento de dados pessoais ocorra, inclusive definindo regras especiais para o tratamento de dados pessoais considerados como sensíveis e para dados de crianças e adolescentes; regras para a transferência internacional de dados; os direitos dos titulares; a definição de responsabilidade de envolvidos no tratamento de dados pessoais (agentes de tratamento); e, sanções administrativas pelo seu descumprimento.

Como característico das leis protetivas de dados de quarta geração, a legislação ainda cria a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Apesar de sancionada em 2018, a LGPD entrou em vigor em sua maior parte apenas em setembro de 2020.

O texto aprovado previa uma *vacatio legis* de 18 (dezoito) meses, mas, principalmente, em razão do despreparo da sociedade civil frente às novas normas, da demora na criação da ANPD pelas autoridades governamentais e da pandemia do novo coronavírus, uma série de medidas legislativas foram tomadas para alterar pontos da LGPD, inclusive o início da sua vigência.

A Medida Provisória nº 959/20 previa a postergação da vigência da LGPD em sua parte mais substancial até 03 de maio de 2021, mas, quando da sua conversão em lei (Lei nº 14.058/20), a previsão foi suprimida, de modo que a vigência das normas protetivas de proteção de dados pessoais iniciou-se no dia seguinte (18 de setembro de 2020) (BRASIL, 2020a).

Um pouco antes, em maio de 2020, o Supremo Tribunal Federal também destacou a tutela jurídica de dados pessoais no ordenamento pátrio – o que, embora não constitua em uma evolução legislativa em sentido formal, merece registro neste breve retrospecto que se está apresentando.

Referendando medida cautelar deferida no bojo das ações diretas de inconstitucionalidade nº 6.387, 6.388, 6.389, 6.390 e 6.393, o plenário do Supremo

Tribunal Federal, por maioria, reconheceu que a proteção de dados pessoais é um direito fundamental.

Os processos discutiam a constitucionalidade da Medida Provisória nº 954/20, que previa o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19).

No histórico julgamento, a medida cautelar proferida pela ministra relatora Rosa Weber, que suspendeu a eficácia da mencionada medida provisória, foi submetida ao referendo do plenário da corte.

Na ocasião, registrou-se que a Constituição Federal prevê um rol de direitos fundamentais da personalidade, concedendo proteção especial à intimidade, à vida privada, à honra e à imagem (art. 5º, inc. X) e, instrumentalizando essa tutela, o art. 5º, inc. XII, da Carta Maior prevê a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (BRASIL, 1988).

Para os ministros, o legislador constituinte defendeu a privacidade individual e a proteção de dados foi garantida expressamente (através da previsão de sigilo de dados) para complementar o direito à intimidade e à vida privada (BRASIL, 2020b).

Para a professora Laura Schertel Mendes, a decisão do Supremo Tribunal Federal reconhece o direito fundamental à proteção de dados pessoais como autônomo, que permite ao tutelado defendê-lo e impõe um dever ao Estado de protegê-lo (MENDES, 2020).

Certamente a decisão do Supremo Tribunal Federal constituiu um importante avanço jurisprudencial no que diz respeito à proteção à privacidade e aos dados pessoais, comparável no direito doméstico à decisão da corte constitucional alemã que, em 1983, estabeleceu pela primeira vez o conceito de autodeterminação informativa no país, servindo de baliza para os debates internacionais sobre a proteção de dados pessoais (MENDES, 2020).

Em harmonia com o entendimento do Supremo Tribunal Federal, em fevereiro de 2022, através da Emenda Constitucional nº 115 (BRASIL, 2022), o direito fundamental à proteção de dados pessoais foi incluído expressamente no art. 5º, inc.

LXXXIX, da Constituição Federal (BRASIL, 1988), tornando-se um direito fundamental, não apenas em sentido material, mas também formal.

A decisão da Corte Suprema e as ainda recentes inovações legislativas, no plano constitucional e infraconstitucional, provocarão grandes debates em torno de seus limites e interpretações, cabendo, principalmente, aos operadores do direito auxiliar nesse trabalho que gera impactos diretos na vida contemporânea.

4 HARMONIZANDO POTENCIAIS CONFLITOS: A PROTEÇÃO DE DADOS PESSOAIS E A IMPORTÂNCIA DE SUA UTILIZAÇÃO

Como visto, é irrefutável que o ordenamento jurídico brasileiro protege os dados pessoais. A decisão do Supremo Tribunal Federal de maio de 2020 demonstra que o Texto Maior já tutelava esse bem jurídico – o que foi reforçado, formalmente, quase dois anos depois pela inclusão expressa no rol de direitos fundamentais do art. 5º da Carta Constitucional, pela Emenda Constitucional nº 115/2022.

Desta forma, não restam mais dúvidas que o art. 2º, inc. I e II, da LGPD, positiva o respeito à privacidade e a autodeterminação informativa com fundamento direto na Constituição Federal.

Contudo, se por um lado se reconhece os dados pessoais como bens jurídicos protegidos e de propriedade de seus titulares, por outro, não se pode olvidar da inegável utilidade que possuem na sociedade informacional.

Não por outra razão, ao lado do respeito à privacidade e da autodeterminação informativa, a LGPD inclui entre os fundamentos da disciplina da proteção de dados pessoais “o desenvolvimento econômico e tecnológico e a inovação” (art. 2º, inc. V) (BRASIL, 2018).

Comentando a previsão legal, Rony Vainzof destaca que “a sociedade que consegue ter a abertura necessária para manipular dados, inovando e gerando novos modelos de negócios, produtos e serviços, automaticamente provoca o desenvolvimento e, consequentemente, alavanca a economia” (VAINZOF, 2021).

Sendo assim, restrições legais ao tratamento de dados são limites a estratégias desenvolvimentistas na economia atual, causando impactos diretos no acesso a novas tecnologias, na promoção de investimentos internacionais e na competitividade de empreendimentos nacionais (GUTIERREZ, 2018, p. 218).

Com a edição da LGPD, criou-se um rol taxativo de hipóteses em que dados pessoais podem ser tratados. Em outras palavras, para que o tratamento de dados pessoais seja considerado legítimo, é preciso que ele se amolde a uma das hipóteses previstas pelo legislador – também conhecidas como “bases legais” (LIMA, 2021).

Este rol está previsto no art. 7º da LGPD, salvo para os dados pessoais considerados como “sensíveis”, cujas bases legais estão previstas no art. 11. Ainda, cabe pontuar que o art. 14 traz algumas previsões especiais para o tratamento de dados pessoas de crianças e adolescentes, considerando a maior vulnerabilidade desse público (BRASIL, 2018).

Em respeito ao objeto delimitado neste estudo, as bases legais para tratamento de dados pessoais em geral, previstas no art. 7º da legislação, terão enfoque.

O rol previsto no mencionado dispositivo contempla dez hipóteses, que incluem, o tratamento fundamentado na obtenção do consentimento do titular, para cumprimento de uma obrigação legal ou regulatória, para o exercício regular de direitos em processo, para a execução de políticas públicas pela Administração Pública, entre outras.

Veja-se, portanto, que aquele que realizará o tratamento de dados pessoais não precisará necessariamente do consentimento do titular, existindo bases legais que legitimam a operação de tratamento ainda que não haja autorização específica do titular. Com efeito, por exemplo, não seria razoável exigir o consentimento do titular para utilizar seus dados em um processo judicial que será movido em face dele.

Esse entendimento é de fundamental relevância para as noções de *data driven business*, pois a definição das estratégias de negócios pode exigir o tratamento de dados pessoais de titulares que não tem um relacionamento prévio com o empreendimento.

Imagine-se, por exemplo, uma organização que pretende conhecer seu mercado em potencial ou mesmo identificar potenciais clientes de seus serviços ou produtos. Na maioria das vezes, os dados que serão tratados são relativos a titulares até então desconhecidos pela organização e que desconhecem a organização, tornando impossível a obtenção prévia de consentimento.

Nesta conjuntura, sem prejuízo da possibilidade de obtenção do consentimento, quando viável, a LGPD prevê duas bases legais que podem ser importantes aliadas às noções de *data driven business*.

A primeira delas encontra-se prevista no art. 7º, inc. IV, que prevê o tratamento de dados pessoais "para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais".

A previsão legal permite que "órgãos de pesquisa", assim considerado o "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico" (art. 5º, inc. XVIII) (BRASIL, 2018), trate dados pessoais independentemente de consentimento para a realização de estudos de caráter histórico, tecnológico ou estatístico (LIMA, 2021).

Assim, a depender da análise de dados a ser realizada, é possível que a utilização desse fundamento legal. Destaque-se, no entanto, que a pesquisa deve ser realizada por um órgão de pesquisa (que pode ser uma pessoa jurídica de direito privado, desde que não possua fins lucrativos) e que há apenas recomendação – e não obrigação – de que os dados sejam anonimizados (isto é, que se utilizem técnicas para que o dado perda a possibilidade de associação a um indivíduo) (LIMA, 2021).

A segunda base legal que merece destaque é a do "legítimo interesse" (art. 7º, inc. IX, da LGPD), estabelecida justamente em razão do reconhecimento da necessidade de bases legais mais flexíveis, que permitam legitimar modelos de negócios inovadores e acompanhar o rápido avanço tecnológico (OLIVEIRA; GONÇALVES, 2020, p. 270).

De acordo com o dispositivo, é lícito o tratamento de dados pessoais "quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (BRASIL, 2018).

O art. 10 da LGPD apresenta brevemente contornos para melhor compreensão da base legal. Segundo o dispositivo, "o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas", admitindo sua

utilização, por exemplo, para “apoio e promoção de atividades do controlador” e para “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” (BRASIL, 2018).

Ainda de acordo com o artigo, apenas os dados pessoais estritamente necessários à finalidade devem ser tratados, o controlador deve adotar medidas para garantir a transparência do tratamento e a ANPD poderá solicitar a apresentação de relatório de impacto à proteção de dados pessoais.

A base não é exclusividade brasileira e é encontrada, por exemplo, no art. 6º, item 1, alínea “f”, da GDPR (UNIÃO EUROPEIA, 2016). Inclusive, na Europa, 70% (setenta por cento) das empresas afirmaram utilizar a mencionada previsão legal para legitimar operações de tratamento (BERBERT, 2019).

Conscientemente estabelecida a base legal, utilizando-se de um conceito jurídico indeterminado (“legítimo interesse”), o legislador garante perenidade à legislação, protegendo os dados pessoais, mas garantindo espaço para o desenvolvimento de soluções inovadoras que eventualmente utilizem esse ativo (OLIVEIRA; GONÇALVES, 2020, p. 277).

A partir da experiência europeia, as autoridades de proteção de dados dos países sujeitos à GDPR sugerem a utilização de um teste de legítimo interesse (“LIA” ou “*legitimate interests assessment*”), que permitirá ao controlador, através de perguntas direcionadas sobre o propósito, a necessidade e a proporcionalidade do tratamento, refletir sobre a existência ou não de um legítimo interesse, frente os interesses envolvidos e as normas legais (REINO UNIDO, 2023).

Neste ínterim, é importante destacar que a dispensa de obtenção do consentimento do titular não exclui a observância à LGPD, devendo as demais normas (como, por exemplo, que tratam dos direitos do titular) serem observadas.

Em termos práticos, ao legitimar uma operação de tratamento de dados pessoais e mesmo não sendo necessário o consentimento, a organização deve possuir uma estrutura apta a atender as demais normas jurídicas protetivas de dados pessoais, não olvidando que o ativo – que pode ser utilizado mesmo sem autorização expressa do titular – continua sendo de sua titularidade.

Ainda que a Lei Geral de Proteção de Dados Pessoais traga maiores responsabilidades ao agente de tratamento (principalmente o controlador), ela não deve ser vista como impedimento ao tratamento de dados pessoais quando,

sopesando interesses envolvidos, prevaleçam o interesse público e/ou o desenvolvimento econômico (sem, contudo, invalidar as garantias fundamentais do titular dos dados).

CONCLUSÕES

O rápido avanço tecnológico aliado ao movimento de digitalização de praticamente tudo, tornando os dados facilmente disponível e processáveis, os tornou um importantíssimo ativo.

A relevância dos dados se tornou tamanha que passaram a ser elemento nuclear de modelos de negócios, produtos, serviços e estratégias empresariais. Os empreendimentos passaram a ser orientados por dados, podendo ser vital para a sustentabilidade dos negócios. Esse fenômeno pode ser resumido à expressão "*data driven business*" e pode se dar através de dados pessoais (informações relativas a pessoas naturais).

Mas, se por um lado, os dados ganharam papel de destaque na sociedade contemporânea, o uso ilimitado de dados pessoais provocou problemas sociais. Invasões na esfera particular do titular dos dados pessoais, inclusive com a possibilidade de utilização para a própria discriminação, exigiram a criação de mecanismos legais que protegessem os indivíduos de tratamentos desarrazoados, principalmente frente a direitos da personalidade, como o da privacidade, intimidade, honra, imagem e vida privada (os quais, no Brasil, são direitos fundamentais).

No cenário brasileiro, a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/18) é o diploma legal que, pela primeira vez e com maior força, passou a tutelar os dados pessoais de forma geral, observando, inclusive, características das legislações mais modernas que tratam a temática no direito comparado.

Para além de estabelecer um rol de direitos do titular em relação aos seus dados pessoais, bem como regras de responsabilização, a legislação limita a licitude das operações de tratamento àquelas que encontrem fundamento nas bases legais previstas pela legislação. Isto é, se o tratamento de dados pessoais não se amolda a uma das hipóteses autorizativas da lei, ele não é ilícito.

Engana-se, no entanto, quem acredita que, a partir da edição da LGPD, o tratamento de dados pessoais só pode ser realizado mediante a obtenção do

consentimento do titular. Além dessa hipótese, a legislação apresenta outras bases legais – algumas dotadas de maior flexibilização.

Nesta conjuntura, o legislador ordinário acertadamente compreendeu que nem sempre será possível ou recomendado obter o consentimento do titular antes do tratamento de eventual dado – o que é de importante valia para as noções de *data driven business*.

Imagine-se o tratamento de dados pessoais com o objetivo de perfilamento ou de prospecção de mercado. Por óbvio, não é possível exigir a obtenção do consentimento do titular antes de realizar um contato comercial ou tentar identificar um mercado em potencial para um novo produto, serviço ou modelo de negócio.

Entrementes, não se pode olvidar que, embora nem sempre o consentimento do titular seja exigível, não se dispensa a obrigação do agente de tratamento observar as demais normas jurídicas previstas na LGPD.

As operações de tratamento de dados pessoais passam a ter maior proteção, inclusive com a criação de mecanismos de defesa pelo legislador, exigindo um posicionamento preventivo e compromissário do agente de tratamento, que deve entender que o titular dos dados é o detentor de tais ativos e tem poder sobre eles.

Os interesses do agente de tratamento e do titular que estejam envolvidos – que, em determinados casos, podem ser conflitantes – devem ser sopesados à luz do caso concreto.

A LGPD não pode e não deve ser interpretada como um obstáculo ao desenvolvimento econômico na sociedade informacional. Apesar de exigir maiores cuidados no tratamento de dados pessoais, não veda ou deve vedar a inovação. Não por outra razão, no seu art. 2º, ao lado de positivar o respeito à privacidade e a autodeterminação informativa, o legislador também destacou a importância e imprescindibilidade do desenvolvimento econômico e tecnológico e da inovação.

REFERÊNCIAS

BAUMAN, Zygmunt. **Vigilância líquida**. Rio de Janeiro: J. Zahar, 2014.

BELL, Daniel. **O advento da sociedade pós-industrial**. São Paulo: Cultrix, 1974.

BERBERT, Lúcia. **“Interesse legítimo” supera “consentimento” no tratamento de dados pessoais pelas empresas**, 2019. Disponível em:

<https://www.telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>. Acesso em: 05 mar. 2023.

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

BÖHMECKE-SCHWAFERT, Moritz; NIEBEL, Crispin. *The General Data Protection's (GDPR) Impact on Data-Driven Business Models: The Case of the Right to Data Portability and Facebook*. **ITU Journal**: ICT Discoveries, n. 2, 9 nov. 2018.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**. Brasília, 5 out. 1988.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**. Rio de Janeiro, 31 dez. 1940.

BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. **Diário Oficial da União**. Rio de Janeiro, 09 ago. 1943.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. **Diário Oficial da União**. Brasília, 15 mar. 2013.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**. Brasília, 11 fev. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**. Brasília, 12 set. 1990.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. **Diário Oficial da União**. Brasília, 15 mai. 1996.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**. Brasília, 10 jun. 2011.

BRASIL. Lei nº 12.529, de 30 de novembro de 2011. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19 de janeiro de 1999; e dá outras providências. **Diário Oficial da União**. Brasília, 01 nov. 2011.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**. Brasília, 15 ago. 2018.

BRASIL. Lei nº 14.058, de 17 de setembro de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020, de 6 de julho de 2020. **Diário Oficial da União**. Brasília, 18 set. 2020.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. **Diário Oficial da União**. Brasília, 17 abr. 2020.

BRASIL. Medida Provisória nº 959, de 29 de abril de 2020. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. **Diário Oficial da União**. Brasília, 29 abr. 2020a.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.387 – Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de jurisprudência**, Acórdãos, 07 mai. 2020b. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf>. Acesso em: 05 mar. 2023.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.388 – Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de jurisprudência**, Acórdãos, 07 mai. 2020b. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949382&ext=.pdf>. Acesso em: 05 mar. 2023.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.389 – Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de jurisprudência**, Acórdãos, 07 mai. 2020b. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950131&ext=.pdf>. Acesso em: 05 mar. 2023.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.390 – Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de jurisprudência**, Acórdãos, 07 mai. 2020b. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950276&ext=.pdf>. Acesso em: 05 mar. 2023.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.393 – Distrito Federal. Relatora: Ministra Rosa Weber. **Pesquisa de jurisprudência**, Acórdãos, 07 mai. 2020b. Disponível em: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950595&ext=.pdf>. Acesso em: 05 mar. 2023.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura; v. 1. 23. ed. rev. e ampl. Rio de Janeiro: Paz e Terra, 2021.

GUTIERREZ, Andriei. Transferência internacional de dados & estratégias de desenvolvimento social. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **Comentários ao GDPR**. São Paulo: Revista dos Tribunais, 2018.

HARTMANN, Philipp Max; *et. al*. *Capturing value from big data – a taxonomy of data-driven business models used by start-up firms*. **International Journal of Operations & Production Management**, v. 36, n. 10, out. 2016, p. 1382-1406.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: Transformação digital: Desafios para o direito. Rio de Janeiro: Forense, 2021.

IKEDA, Kazuaki; MARSHALL, Anthony; MAJUMDAR, Abhijit. ***More than magic***: *How the most successful organizations innovate*, 2016. Disponível em: <https://www.ibm.com/downloads/cas/BDZ5NPLE>. Acesso em: 05 mar. 2023.

LIMA, Caio César Carvalho. Capítulo II – Do tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord.). **LGPD**: Lei Geral de Proteção de Dados comentado [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

MENDES, Laura Schertel. **Decisão história do STF reconhece direito fundamental à proteção de dados pessoais**, 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em: 05 mar. 2023.

MIELE, Susan; SHOCKLEY, Rebecca. ***Analytics***: *The real-world use of big data*, 2013. Disponível em: <https://www.informationweek.com/pdf_whitepapers/approved/1372892704_analytics_the_real_world_use_of_big_data.pdf>. Acesso em: 05 mar. 2023.

NADER, Paulo. **Introdução ao estudo do direito**. 36. ed. Rio de Janeiro: Forense, 2014.

OLIVEIRA, Dânton Hilário Zanetti de; GONÇALVES, Luís Felipe Pilagallo da Silva Mäder; VALASKI, Luís Henrique. Consentimento e legítimo interesse como hipóteses de tratamento de dados pessoais na Lei Geral de Proteção de Dados (Lei nº 12.709/2018): Paradoxos e convergências. In: FARIA, Mariana Pereira; SILVA, Rafael Aggens Ferreira da; GOMES, Rhodrigo Deda (Coord.) **Direito e inovação**. v. 3. Curitiba: OABPR, 2020.

PINHEIRO, Patricia Peck. **Direito digital**. 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/18 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

REINO UNIDO. Information Commissioner's Office (ICO). ***Legitimate interests****: How do we apply legitimate interests in practice?* Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>. Acesso em: 05 mar. 2023.

SEMIDÃO, Rafael Aparecido Moron**. Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da ciência da informação**: Contribuições teóricas. Dissertação (Mestrado em Ciência da Informação) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2014.

THE GUARDIAN. ***Revealed***: *50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em 05 mar. 2023.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L 119/1, 04 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 12 mar. 2023.

VAINZOF, Rony. Capítulo I – Disposições preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). **LGPD**: Lei Geral de Proteção de Dados comentado [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.