UNIVERSIDADE NOVE DE JULHO

DEPARTAMENTO DE PÓS-GRADUAÇÃO *STRICTO SENSU*

PROGRAMA DE MESTRADO EM DIREITO

MATEUS LUCATTO DE CAMPOS

A REGULAÇÃO DA ATIVIDADE EMPRESARIAL EM RELAÇÃO À COLETA, USO E TRATAMENTO DE DADOS

São Paulo

2023

UNIVERSIDADE NOVE DE JULHO

DEPARTAMENTO DE PÓS-GRADUAÇÃO *STRICTO SENSU*

PROGRAMA DE MESTRADO EM DIREITO

A REGULAÇÃO DA ATIVIDADE EMPRESARIAL EM RELAÇÃO À COLETA, USO E TRATAMENTO DE DADOS

Dissertação de Mestrado apresentada à banca examinadora da Universidade Nove de Julho, como requisito parcial para obtenção ao título de **MESTRE** em Direito, sob a orientação do Profa. Dra. Renata Mota Maciel.

São Paulo

2023

Campos, Mateus Lucatto de.
A regulação da atividade empresarial em relação à coleta, uso e tratamento de dados. / Mateus Lucatto de Campos. 2023.
112 f.

Dissertação (Mestrado) - Universidade Nove de Julho - UNINOVE, São Paulo, 2023.
Orientador (a): Profª. Drª. Renata Mota Maciel.

1. Empresa. 2. Privacidade. 3. Proteção de dados pessoais. 4. Poder econômico.
I. Maciel, Renata Mota. II. Título.

CDU 34

MATEUS LUCATTO DE CAMPOS

A REGULAÇÃO DA ATIVIDADE EMPRESARIAL EM RELAÇÃO À COLETA, USO E TRATAMENTO DE DADOS

Dissertação apresentada ao Programa Pós-Graduação Stricto Sensu em Direito da Universidade Nove de Julho como parte das exigências para a obtenção do título de Mestre em Direito.

São Paulo, 07 de dezembro de 2023.

BANCA EXAMINADORA

Profa. Dra. Renata Mota Maciel
Orientadora
UNINOVE

gov.br
Documento assinado digitalmente
SAMANTHA RIBEIRO MEYER PFLUG MARQUES
Data: 08/12/2023 15:17:39-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Samantha Meyer-Plug Marques
Examinadora Interna
UNINOVE

MARIA RITA REBELLO PINHO DIAS:28337104880
Assinado de forma digital por MARIA RITA REBELLO PINHO DIAS:28337104880
Dados: 2023.12.07 22:27:25 -03'00'

Profa. Dra. Maria Rita Rebello Pinho Dias
Examinadora Externa
EPM

AGRADECIMENTOS

Dedico este trabalho em primeiro plano à Deus e à minha família. Sem a figura de meus pais, João Lúcio Cruz de Campos e Marilda Aparecida Lucatto de Campos, e de meus irmãos, João Lúcio Lucatto de Campos e Luciana Lucatto de Campos, não lograria êxito nas atividades profissionais e acadêmicas. Sou ainda grato a Deus e à minha família pois são eles o suporte nos momentos agradáveis e nos difíceis, ínsitos à caminhada de qualquer espírito.

Agradeço, ainda, à minha orientadora profa. Dra. Renata Mota Maciel, pelos anos de pesquisa e orientação. Sem o auxílio da nobre professora eu não teria o subsídio necessário para crescimento e evolução.

Por fim, agradeço à colega e professora Carolina Tavares de Carvalho, que muito me auxiliou no desenvolvimento e organização das minhas ideias, e na introdução às técnicas acadêmicas que viabilizaram o raciocínio desenvolvido.

RESUMO

A transmissão de dados pessoais é fenômeno indissociável da vida no atual estágio da sociedade. Para a realização de compras, obtenção de serviços e até efetivação de reclamos e pleitos é por vezes necessário que se informem dados que dizem respeito apenas ao titular. Com o advento da sociedade da informação e do incremento das práticas de comércio eletrônico, tornaram-se as empresas em verdadeiras gestoras de bancos de dados de significativa extensão. Com a posse desses materiais, é possível às instituições detentoras a prática de atos como envio indesejado de publicidade, imposição de fornecimento de dados para obtenção de serviços sem necessidade, assédio a consumidores que e exercício de influência no comportamento de terceiros, valendo-se do poder que as informações proporcionam. Assim, em acordo ao percurso do tratamento legislativo da proteção de dados no Brasil, é necessário que se compreenda melhor a tarefa da regulação nessa seara, vez que a perspectiva puramente contratualista não pode tutelar o cidadão diante de práticas nocivas empreendidas pelas empresas quanto aos dados pessoais. Nesse contexto, foi aprovada a Lei 13.709 de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento dessa gama de dados. No entanto, a regulação e autuação empreendidas pelos órgãos competentes ainda é escassa quando em comparativo principalmente com a União Europeia, e problemas relacionados a tratamento indevido de dados ainda desaguam nos tribunais. Sendo assim, para a sua eficiência, é necessário investigar a regulação e a aplicabilidade de legislações e regulamentos similares em outros países com histórico de proteção de dados, em conjunto com o que está ocorrendo no Brasil, visando prevenir violações aos direitos dos titulares de dados, preventivamente. Em passo seguinte, a aproximação com o modelo regulatório europeu, com maior concretude, bem como o implemento de ferramentas autorregulatórias, como o compliance, podem se mostrar úteis no desiderato de proteção de dados pessoais, considerando que a realização do objeto social não mais basta às empresas, sendo de rigor a conformidade com as normas e o respeito ao indivíduo. Para tanto, utiliza-se o método hipotético-dedutivo, com auxílio de pesquisa bibliográfica como procedimento metodológico. Como hipóteses, tem-se que: 1) a implementação do modelo regulatório europeu de proteção de dados pode contribuir para a eficácia da LGPD, potencialmente reduzindo litígios entre indivíduos e empresas que utilizam dados como ativos; 2) a incorporação de mecanismos autorregulatórios é uma abordagem adequada tanto para salvaguardar os direitos do titular dos dados, ao minimizar a dependência de recursos externos, quanto para promover um ambiente alinhado com a LGPD e mais equitativo entre os atores econômicos, favorecendo uma simetria de informações entre empresas e tornando a busca por dados menos intrusiva. O tema se insere na área de concentração do programa de Mestrado e Doutorado da (PPGD) da Uninove que é “Direito Empresarial: Estruturas e Regulação”, com linha de pesquisa em “empresa transnacional e regulação”.

PALAVRAS-CHAVE: Empresa. Privacidade. Proteção de Dados Pessoais. Poder Econômico.

ABSTRACT

The transmission of personal data is an inseparable phenomenon of life in the current stage of society. In order to make purchases, obtain services and even make claims and pleas, it is sometimes necessary to provide data that only concerns the holder. With the advent of the information society and the increase in e-commerce practices, companies have become true managers of databases of significant size. With the possession of these materials, it is possible for the institutions that hold them to practice various acts and influence the behavior of third parties, taking advantage of the power that the information provides. Thus, in accordance with the evolution in the legislative treatment of data protection, it is necessary to better understand the task of regulation in the field of data, since the purely civil and contractual perspective is not able to protect the citizen against harmful practices undertaken by companies regarding personal data, beyond the classic examination of contractual freedom. In this context, law 13.709 of August 14, 2018, called the General Law of Personal Data Protection (LGPD), was approved, which provides for the treatment of this range of data. However, the regulation and enforcement undertaken by the competent bodies is still scarce when compared mainly with the European Union, and problems related to improper data processing still end up in the courts. Therefore, in order to be effective, it is necessary to research the regulation and applicability of similar laws and regulations in other countries with a history of data protection, in comparison with what is also happening in Brazil, with the aim of preventing violations of the rights of data subjects from occurring in the first place. As a next step, a closer relationship with the European regulatory model, with greater concreteness, as well as the implementation of self-regulatory tools, such as compliance, may prove useful in the pursuit of personal data protection, considering that the realization of the corporate purpose is no longer enough for companies, and compliance with the rules and respect for the individual are rigorous. To this end, the hypothetical-deductive method is used, with the aid of bibliographical research as a methodological procedure. The hypotheses are that: 1) the European regulatory paradigm for data protection can be useful for the efficiency of the LGPD, with possible repercussions in reducing litigation by individuals against companies that use data as assets; 2) the adoption of self-regulatory instruments is a suitable tool both for the protection of the individual who holds the data, since it reduces the need to resort to external means of protection, and for the generation of an environment that is consistent with the LGPD and more equitable between economic agents, since information will tend to be more symmetrical between companies and its search less invasive. The topic is part of the area of concentration of Uninove's Master's and Doctorate program (PPGD), which is "Business Law: Structures and Regulation", with a line of research on "transnational companies and regulation".

KEYWORDS: Company. Privacy. Protection of Personal Data. Economic Power.

SUMÁRIO

INTRODUÇÃO

É notável que para qualquer simples ato a ser empreendido presentemente é exigido que informemos dados de cunho pessoal. Caso se deseje obter um esclarecimento, comprar um remédio, adquirir um alimento, presentear um ente familiar, pagar por um serviço desejado, realizar um curso, por vezes somos obrigados a transmitir às instituições com quem temos contato dados que nos dizem exclusivo respeito. A própria vida em sociedade, nesses termos, exige a transmissão de dados. Assim, para além da assinatura e cumprimento dos contratos que desejamos firmar, resta sempre a dúvida sobre o uso que será feito dos dados repassados.

Notícias frequentes sobre vazamentos, como o incidente de segurança envolvendo informações pessoais das chaves PIX em janeiro de 2022 no Brasil, a operação *Deepwater* da Polícia Federal em 2021, sobre dados vazados em fórum de internet, e o notório caso Edward Snowden, que expôs possível vigilância de cidadãos por meio de bancos de dados de grandes empresas, demonstram que as informações provenientes desses vazamentos têm um valor significativo. Esses eventos ressaltam a importância das informações derivadas de dados sensíveis.

Ademais, com o advento da pandemia, as transações efetuadas em ambiente eletrônico tornaram-se mais recorrentes ainda, assim como a transferência de dados a elas correlatas. E, nesse cenário de sociedade informacional, é que foi criada a Lei Geral de Proteção de dados (LGDP), promulgada em 14/08/2018 e vigente em sua completude em 01/08/2021 (art. 65).

De ordinário, ainda se recorre à tradição civilista para resolução de problemas que ocorram com instituições empresariais, usualmente com resolução perante o Poder Judiciário por intermédio dos instrumentos processuais. Questões como inadimplemento absoluto ou relativo, atrasos, cobranças por dívidas já pagas, vícios na vontade, dentre outros, são levadas a debate e às cortes de Justiça, trazendo por usuais parâmetros as legislações sobre direito das obrigações e contratos.

No entanto, problemáticas como envio indevido de publicidade sem consentimento; falta de informações quanto ao uso de dados requisitados; imposição de aceitação de cookies em sítios eletrônicos; envio de dados coletados por empresas a outras empresas; uso de métodos impositivos e obscuros para coleta de dados, tais como requisição de informações adicionais para leitura de propostas, atualização de aplicativos ou deferimento de isenções/ofertas que influenciem no valor do produto/serviço; requisição de dados desnecessários; possível indução de comportamento das pessoas com base em dados sensíveis (especialmente idosos) e em

anúncios personalizados; além de vigilância indevida a partir de dados de rotina, não guardam direta relação com tais institutos, pois por vezes ocorrem no mesmo contexto de uma prestação contratual que, em âmbito formal, foi assinada e se tornou vigente.

Nesse panorama, conquanto existente uma lei protetiva de dados, inexiste um ambiente que proveja uma suficiente proteção de cidadãos expostos a práticas agressivas de mercado por parte dos agentes econômicos, principalmente no que tange às instituições financeiras e empresas de telefonia. Tal insuficiência contribui, ao menos em parte, para a não resolução dos problemas com as pessoas, que terminam por buscar o Judiciário.

Por estas perspectivas, elabora-se a seguinte pergunta: que meios podem ser utilizados para intensificar a eficiência da LGPD na proteção de dados das pessoas expostas às práticas empresariais, especialmente no que tange à busca por novos clientes, diminuindo a litigiosidade perante Tribunais?

Neste sentido, a hipótese é a de que a aproximação de nosso modelo regulatório de proteção de dados ao modelo europeu pode contribuir para aumento da proteção dos cidadãos e diminuição da litigiosidade. Assim, torna-se imprescindível a análise das questões associadas à salvaguarda de dados em nações com experiência nesse domínio, notadamente entre os integrantes da União Europeia, bem como as deliberações já discutidas e deliberadas no contexto brasileiro. Isso visa extrair ensinamentos e padrões de conduta a serem adotados pelas organizações e empresas locais, com o intuito de prevenir potenciais transgressões aos direitos vigentes.

Por sua vez, o objetivo geral é examinar o efetivo avanço ou não da LGPD no que tange ao respeito aos direitos dos titulares de dados por parte de empresas que utilizam dados como ativos para suas atividades. Afinal, para viver em sociedade, nos moldes atuais, é necessária a permanente disponibilização de dados de cunho pessoal, sendo necessário o exame da real proteção dispensada aos cidadãos.

Além disso, nossos objetivos específicos são: a) examinar demandas judiciais envolvendo ofertas abusivas e uso irregular de dados dos cidadãos para verificar se a LGPD tem contribuído para diminuição da litigiosidade ou não; b) identificar os meios pelos quais seria possível intensificar a eficiência da LGPD na diminuição dos conflitos; e c) estabelecer comparativos com a experiência regulatória europeia para identificação de paradigmas passíveis de adoção no Brasil.

Para enfrentar as questões objeto de reflexão, o trabalho é estruturado em três capítulos.

O início do estudo investiga a transformação no manejo de dados conforme as leis brasileiras até a implementação da LGPD. Essa análise abrange a evolução do valor atribuído

aos dados pelo legislador e as estratégias de gestão, visando uma compreensão mais aprofundada de um modelo eficaz para prevenir violações de direitos, especialmente durante a coleta de dados por agentes econômicos. Neste capítulo, é analisada a transformação no manejo de dados, ressaltando a crescente importância atribuída pelos legisladores e as táticas de administração viabilizadas por leis específicas. Tudo isso visa alcançar um modelo mais eficaz na prevenção de violações de direitos durante a coleta de dados por entidades econômicas.

O segundo capítulo tem, em um primeiro momento, a finalidade de analisar algumas das decisões emanadas dos órgãos europeus responsáveis pela tutela de direitos dos titulares de dados pessoais. Considerando a experiência europeia com legislação nesse sentido, a forma de atuação dos órgãos pertinentes, bem como as razões utilizadas nos procedimentos relativos às empresas que violaram direitos relacionados a dados pessoais, têm pertinência para aplicação no Brasil. Além disso, busca-se a análise de decisões proferidas também no Brasil, bem como a verificação da suficiência ou não da tutela estatal até então empreendida para proteção de direitos previstos na LGPD, em comparativo com o desenvolvimento no continente europeu.

Por fim, no terceiro capítulo, destacamos as vantagens resultantes da aproximação do nosso conjunto de regras com o europeu. Detalhamos instrumentos e abordagens já implementados em um continente mais experiente nessa área, visando reduzir disputas que poderiam ser evitadas caso a LGPD fosse efetivamente observada. Em um segundo momento, com atenção ao âmbito interno das empresas, indicamos instrumentos de autorregulação idôneos para o auxílio às empresas no que tange à prevenção dos ilícitos em prejuízo dos detentores de dados. *Compliance*, estudos de impacto, *privacy by design*, são avaliados como potenciais antídotos a práticas que nos últimos anos tem sido identificadas como lesivas aos cidadãos, que poderiam ser cerceadas antes mesmo da provocação de órgãos competentes para análise do tema proteção de dados.

Esta pesquisa é inerente ao tema Empresas e Direitos Humanos, o qual, encontra-se inserido na Área de Concentração “Direito Empresarial: Estruturas e Regulação”, desenvolvida no Programa de Pós-Graduação *Stricto Sensu* em Direito da Universidade Nove de Julho (UNINOVE).

Em desfecho, quanto às técnicas de pesquisa, este trabalho utiliza o método hipotético-dedutivo, e como procedimento metodológico a revisão bibliográfica e documental.

1 A EVOLUÇÃO DO TRATAMENTO DE DADOS NA EXPERIÊNCIA BRASILEIRA

1.1 Economia e Sociedade da Informação

Antes de avaliar a específica gestão de dados no país e sua evolução até os patamares atuais, é necessário examinar a relevância dos dados na prática empresarial em acordo às informações e conhecimentos que a posse deles pelos agentes econômicos proporciona. Nesse desiderato, dentre os estudos relacionados à microeconomia, ramo que basicamente se direciona à análise das tomadas de decisão por famílias e empresas e suas respectivas interações em mercados específicos, encontra-se a "economia da informação" ou "economia da informação assimétrica". Dado que algumas pessoas ou organizações possuem maior conhecimento sobre uma relação, fenômeno conhecido como "assimetria de informações", esta área de pesquisa se concentra na análise do impacto dessa diferença de compreensão e discernimento sobre as decisões tomadas por pessoas e organizações, bem como na dinâmica interna das relações estabelecidas entre elas.

Assim, Mankiw (2020, p. 364) introduz o tema:

> Eu sei algo que você não sabe.' Essa provocação é comum entre crianças, mas também traduz uma verdade profunda a respeito de como as pessoas interagem umas com as outras em algumas situações. Em muitas situações da vida, uma pessoa sabe mais do que outra sobre o que está acontecendo. Uma diferença de acesso a conhecimento relevante é chamada informação assimétrica.

Entre os paradigmas utilizados (MANKIW, 2020) para raciocínio se encontra a possibilidade de que um trabalhador saiba mais sobre o valor de seu trabalho do que o patrão, o que se denomina de "ação oculta", em que uma das partes que não detém a informação relevante gostaria de tê-la. A problemática resultante desse contexto é o "risco moral" que surge quando um agente (a exemplo do funcionário) realiza uma tarefa em nome de outrem, chamado de principal (exemplo do patrão). Nesse panorama, se o principal (patrão) não detiver meios para fiscalizar adequadamente o comportamento do agente (funcionário) há o risco de que o encarregado não empregue seus melhores esforços segundo o esperado (risco de comportamento imoral ou inadequado). Os principais (patrões) poderiam, dentre outros, criar uma melhor fiscalização, oferecer incentivos como o aumento de salários e o adiamento do pagamento de benefícios, a fim de aumentar o período de fiscalização, com chances de perda em caso de infrações, e usar mecanismos para diminuir o risco moral. Nas administrações

corporativas de empresas de capital aberto, ocorrem problemáticas semelhantes. Nesse contexto, os interesses dos acionistas (principal) frequentemente entram em conflito com os objetivos dos administradores (agente), os quais possuem informações mais detalhadas sobre os negócios. Um exemplo é a possibilidade de os administradores buscarem, não necessariamente, a maximização dos lucros desejada pelos acionistas, mas sim interesses pessoais. A existência de um conselho diretor e de órgãos deliberativos tem também como finalidade a monitoração da harmonia dos distintos interesses.

A assimetria de informação pode atingir igualmente a relação entre vendedores e compradores, ou fornecedores e consumidores, oportunidades em que uma das partes pode terminar não tomando a melhor decisão em razão da falta de informações suficientes. Em um exemplo, podemos citar o caso de um comprador de um bem, como uma casa ou um eletrodoméstico, que adquire o produto com algum defeito específico sem conhecimento prévio, e paga um valor mais elevado do que pagaria se tivesse essa informação. Além disso, há a situação em que uma seguradora oferece seguro de vida a um indivíduo sem estar ciente de que ele é fumante, indicando uma expectativa de vida menor, caracterizando fenômenos conhecidos como “seleção adversa”. Samuelson e Nordhaus (2012) afirmam que solucionar a assimetria de informação é um dos motivos para o uso de regulação das atividades econômicas pelos países, na finalidade última de evitar efeitos nocivos de práticas monopolistas. Assim sendo, é sobremaneira relevante adquirir informações, afinal elas podem influenciar a tomada de decisões acerca de investimentos e operações, bem como é igualmente importante que se evite desequilíbrio na posse das mesmas informações, com vistas à preservação de um ambiente concorrencial harmônico.

Dentro desse cenário, Frank e Bernanke (2012) observam que, na perspectiva da teoria da mão invisível de Adam Smith, que favorece uma menor intervenção do Estado e a autorregulação do mercado, há a suposição de que os agentes possuem um nível adequado de informação para conduzir suas atividades e tomar decisões de gastos e investimentos. Contudo, argumenta-se que essa premissa é infundada, uma vez que é pouco plausível acreditar que tanto indivíduos quanto empresas estejam sempre completamente informados sobre todos os aspectos relevantes.

As informações provenientes de dados, consequentemente, são deveras importantes para a atividade de um empresário ou empresa, ao ponto de Frank e Bernanke (2012, p. 360) afirmarem que “sem dúvida, ter mais informações é melhor que ter menos, mas, em geral, custa caro adquiri-las”, e que a tarefa de “obtenção de informações é uma atividade como qualquer outra”.

Um efeito direto da existência de agentes mal-informados é o de que, para além do contexto de uma boa ou má decisão tomada, “muitas transações potencialmente benéficas são impedidas de se realizar em função de informações assimétricas – que uma parte não dispõe das informações que a outra parte dispõe” (FRANK; BERNANKE, 2012, p. 376). Em exemplo concreto, assim refletem:

> Por exemplo, o proprietário de um carro usado sabe se ele está em boas condições, mas os potenciais compradores não sabem. Embora um comprador pudesse estar disposto a pagar mais por um bom carro do que o seu proprietário exigiria, o fato de que o comprador não pode ter a certeza de estar comprando um bom carro muitas vezes desencoraja a venda. De maneira geral, a infor- mação assimétrica geralmente impede os vendedores de oferecer o mesmo nível de qualidade pelo qual os consumidores estariam dispostos a pagar. (FRANK; BERNANKE, 2012, p. 376).

Enfim, em qualquer atividade de cunho empresarial é fundamental a obtenção de informações.

Benacchio e Maciel (2020) chegam a afirmar que, dado o desenvolvimento da tecnologia de obtenção de informações pessoais e do marketing, com amplificação do conhecimento dos comportamentos dos consumidores, criou-se ambiente apto a melhor “monetizar dados de forma cada vez mais elaborada” (BENACCHIO; MACIEL, 2020, p. 46), tornando os dados um verdadeiro material precioso, com “inegável expressão econômica, sendo um vetor importante no funcionamento na chamada economia da informação” (DE LUCCA; MACIEL, 2019, p. 28). Mediante o conhecimento proporcionado pelos dados, decide-se melhor sobre qual ramo investir, qual espécie de consumidor buscar e a quem oferecer produtos e serviços, buscando ao final a melhor vantagem para ambos segundo o interesse que cada qual detenha. Por óbvio, as informações podem ser obtidas mediante o acesso a dados pessoais relacionados a consumidores/compradores, afinal o conhecimento sobre o público responsável pela compra dos produtos e serviços é crucial. Assim sendo, existindo uma lei específica sobre tratamento de dados pessoais, é fundamental que se tenha ciência e reflexão mínimas sobre os possíveis impactos dela na atividade empresarial e gestão de dados. Além de destacar a importância dos dados e suas implicações para o funcionamento da empresa, conforme estudado pela economia da informação, as características atuais da sociedade permitem concluir que os dados são matéria-prima essencial e um componente inseparável das atividades de interação. Esse cenário é especialmente relevante nas ações de natureza econômica no ambiente em que vivemos.

De acordo com De Lucca e Maciel (2019), o desenvolvimento da tecnologia tem

impulsionado progressivamente a temática de proteção de informações pessoais. Eles argumentam que, embora a proteção de dados não seja uma preocupação recente, foi a partir do advento da Sociedade do Conhecimento que a proteção normativa se tornou uma prioridade evidente (DE LUCCA, MACIEL, 2019, p. 27).

Lisboa (2020), em avaliação do termo "sociedade da informação" a partir do exame da situação do Japão pós-guerra (a partir de 1945), explica que com o término da segunda gerra mundial os Estados Unidos empreenderam políticas de auxílio ao país do oriente, diante dos nocivos resultados do litígio. Através desse suporte mencionado, ocorreu um notável avanço econômico, porém, não foi acompanhado pelo desenvolvimento de outros setores relacionados à infraestrutura. Isso abrange políticas de urbanização e habitação, impactos ambientais do crescimento econômico, organização do setor viário, avanço sanitário e dos espaços públicos, além da falta de acesso a bens básicos, entre outros desafios. Tal panorama gerou debates e reflexões nos meios acadêmico e político, com foco na melhoria do acesso da população a distintos recursos. A "sociedade industrial", em todos os seus setores, apresentava a necessidade de desenvolvimento tecnológico e de aumento da competitividade, tendo por ponto comum o valor econômico da informação, a possibilitar maior coerência, unicidade e civilidade aos processos de crescimento que, doravante, necessitam de dados e de seu compartilhamento. Assim menciona o autor (LISBOA, 2020, p. 29):

> Tadao Umesao propôs a *teoria da informação como fenômeno social*. Tendo por premissa que a sociedade industrial havia sido superada por uma nova era, a qual designou *indústria da informação ou sociedade da informação*, o professor de Kyoto afirma que a sociedade da informação é um *sistema social coerente* e, portanto, deve ser tratado como *teoria civilizatória* modificadora da relação interpessoal e da coletividade pela utilização de tecnologia fundamentada no *compartilhamento de dados*. Isso pressupõe uma mudança de paradigma a ser adotado: se na guerra, é normal o segredo e o buscar incessante do que se conhece sobre o seu inimigo, a sociedade da informação pressupõe a paz e a concorrência leal. Nesse ambiente, o compartilhamento da informação possibilita a redução espacial e de tempo para que as interações sociais possam ocorrer em maior quantidade e, preferencialmente, com melhor qualidade.

Sem descurar os estudos americanos sobre processamento e compartilhamento de dados por computadores, Lisboa (2020) indica que a modernização do Japão nesse período pós-guerra passou pela adoção dos pensamentos e práticas relacionados à teoria da informação, pois a sociedade nela (informação) baseada impulsionaria os serviços prestados, os contratos, os esportes, a cultura e o lazer em intensidade sem precedentes. Nesse contexto, da era das máquinas se passou à era do conhecimento, com maior interação e superação de

individualismo. Pesquisas e práticas obtidas de empresas e universidades americanas e europeias conjugadas com universidades e empresas do Japão conferiram *know-how* e viabilizaram a concorrência internacional. O sucesso das pesquisas levou o país ao aumento da exportação, redução de preços, maior produção e desenvolvimento de diferentes setores, a incluir o “chip” com função de microprocessador, em avanço permitido aos usuários de computador, além da biotecnologia. A informação superou o *status* de dado relacionado à defesa de estado para o uso em proveito da sociedade, e seu compartilhamento aproveitado para interesses sociais, qualidade de vida, saúde, educação, lazer, entre outros.

O governo japonês elaborou um plano para uma sociedade de informação, cujo relatório final foi emitido em 1972. Nesse documento, conferiu-se valor econômico e social à informação, destacando características como preferência por "ações informacionais" em detrimento das industriais. Além disso, enfatizou-se a melhoria da capacidade e qualidade dos softwares para reorganizar os sistemas sociais, integrando-os aos subsistemas decorrentes (LISBOA, 2020, p. 37). Essas medidas buscavam promover maior acessibilidade ao computador, possibilitando uma interação mais expressiva entre indivíduos, universidades, governos, comércio e a coletividade em geral. Isso representou um "alargamento" da infraestrutura em direção a uma indústria do conhecimento.

Segundo Santos (2002, p. 11), a "revolução das tecnologias e práticas de informação e comunicação" integra-se ao contexto da globalização. Martins (2020, p. 162) destaca duas características principais dessa dinâmica de organização social: o aumento na criação, transmissão e circulação de conhecimento, informações e ideias/doutrinas, e a valorização econômica dos bens imateriais ligados ao conhecimento em níveis superiores aos bens materiais.

. Quanto ao primeiro contexto, indica que o avanço da tecnologia e da internet representou realidade que arrefeceu fronteiras entre pessoas, países e meios de comunicação, com expansão de conhecimento e ideias por variadas formas que não apenas o papel. Além disso, bens imateriais ligados ao conhecimento passaram por vezes a ter mais valor do que os bens materiais produzidos a partir desses conhecimentos (a exemplo de marcas, patentes, entre outros), a ponto de ser possível se falar em ativo de natureza intelectual. Todo esse panorama, ademais, insere-se em um enredo que ostenta desenvolvimento de mecanismos de armazenamento de dados eletrônicos, com aumento inclusive da possibilidade de uso das informações para propósitos distintos aos enunciados como justificativa para sua coleta: “a questão, portanto, muito além da disponibilização pública de dados, já existente há muito tempo, é a facilidade de sua coleta, uso e abuso por parte do detentor da informação” (DEZEM;

DE LUCCA, 2018; p. 13).

Em desfecho, adquirir dados, segundo estudos econômicos, é fundamental ao exercício de qualquer atividade empresarial, afinal eles viabilizam o conhecimento necessário à tomada das melhores decisões. Essa necessidade, inserida em contexto atinente à sociedade da informação, torna-se ainda mais relevante porquanto a atuação de qualquer empresa estará necessariamente envolvida em ambiente no qual a informação e o conhecimento (originados dos dados) são ativos indissociáveis para qualquer atividade. Assim sendo, se parte dos dados necessários à atuação da empresa é de natureza pessoal, e se há legislação no Brasil (baseada principalmente na experiência europeia) que trata dos dados pessoais, qual seja a lei 13.709 de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD), é de rigor o estudo do impacto dessa lei nas atividades empresariais, tomando como base o vivenciado em países com maior histórico de debate sobre a proteção deles, e também em acordo aos estudos sobre a própria natureza desses elementos. Para tanto, em primeiro plano, é fundamental que se examinem as origens da proteção jurídica conferida aos dados.

1.2 Origens do Direito à Privacidade e conteúdo ético da proteção de dados

O indivíduo deve ser protegido. Sobre tal proposição repousam os ordenamentos e seus respectivos instrumentos, com primordiais vistas à tutela de seu corpo e propriedade. No entanto, ao menos desde o século XIX, há a compreensão de que a proteção ao indivíduo não deve compreender apenas a proteção de sua pessoa física e de seu patrimônio contra as agressões. Warren e Brandeis (1890), em reconhecido artigo denominado "The Right to Privacy", publicado na Harvard Law Review e importante matriz do reconhecimento ao direito de privacidade, pontuam que as mudanças políticas, sociais e econômicas implicam o reconhecimento de novos direitos, havendo o sistema jurídico de permanecer atento às novas demandas. Dezem e De Lucca (2018), em exame ao texto, mencionam que anos antes da publicação do artigo de Waren e Brandeis surgiram inovações tecnológicas que conduziram os juristas a novas reflexões acerca da proteção de bens que não são tangíveis.

Dentre as novidades, encontravam-se à época a popularização da fotografia[1] e o advento de empreendimentos de cunho jornalístico, fatos esses que tornaram as informações de cunho pessoal acessíveis a terceiros em patamares substancialmente inéditos para os parâmetros até

[1] Fundação da "Eastman Kodac Company" em 1.888 por George Eastman (disponível em: https://pt.wikipedia.org/wiki/Kodak. Acesso em 14/08/2023).

então conhecidos.

Nesse contexto, Warren e Brandeis argumentaram que ao longo do tempo ocorreu a identificação inevitável de uma extensão imaterial da personalidade. Essa abordagem engloba aspectos não estritamente materiais, como sentimentos e intelecto, resultando na previsão de direitos como propriedade intelectual, o direito de desfrutar da vida com liberdade e o direito de ser deixado em paz. Além disso, destacaram a importância da proteção de bens jurídicos também imateriais, como obras de literatura e arte.

Em raciocínio indutivo, refletiram que da inconteste imprescindibilidade de punição em razão de uma lesão física à pessoa, considerando uma análise histórica da progressão da proteção, num momento seguinte também se mostrou como necessária a punição em decorrência de uma simples ameaça de lesão (e ao temor psicológico em si que ela invariavelmente gera), bem como da direta proteção ao corpo, se estendeu igualmente a proteção em face dos sofrimentos "indiretos" gerados por poluição sonora e visual, invasão à intimidade do lar e ofensas à reputação do indivíduo perante os outros cidadãos (crimes de calúnia e difamação).

Em outras palavras, com o advento da vida em sociedade, inevitável é o desenvolvimento das leis que a regem. Conforme destacam, apenas parte de nossas experiências, tanto as dolorosas quanto as prazerosas, está relacionada a bens estritamente materiais, que têm sido historicamente o foco das preocupações legislativas, como o direito de propriedade. Diante disso, as autoridades precisam reconhecer a necessidade de tutelar não apenas o que é tangível, mas também tudo que envolve o indivíduo, incluindo dados que revelam seus pensamentos, emoções, sensações, preferências e estilo de vida, levando juristas a refletirem sobre a existência de princípios aplicáveis a essa proteção. Do contrário, em ilustração ao potencial contrassenso da desatenção do direito às facetas da vida em sociedade que guardam conexão com a proteção do indivíduo em si, dissertam que seria permitido às empresas de informação que devassassem o que ocorre no interior de um lar para o público, bastando para isso que não caluniassem ou difamassem os moradores.

Ou, no mesmo passo, que se utilizasse inadvertidamente a imagem das pessoas tendo por vetor final apenas os interesses financeiros de um explorador, sob a falsa justificativa de que desses atos não decorre lesão física ou patrimonial direta aos envolvidos. Em exemplificação mais concreta desenvolvida no trabalho, aduzem que seria pouco defensável perante um ordenamento a conferência de um direito a alguém para publicar uma espécie de inventário ou catálogo acerca de bens preciosos que uma pessoa possui em sua casa, mesmo que sem prejuízo direto. Se adotado, aliás, comparativo de relevância afora o valor monetário,

retratam que o esforço desenvolvido em uma vida, com suas consequentes nuances (informações, rotina, pensamentos, decisões), são por vezes maiores do que o esforço para produzir um texto, um poema ou uma pintura, esses sim que por serem interpretados como extensão de um direito de propriedade (atualmente "direito autoral"), auferem eficaz e inquestionável tutela estatal contra tratamentos indevidos.

Dessa forma, em debate acerca do conteúdo de um direito à privacidade há de se pontuar como núcleo o respeito ao indivíduo, às suas relações familiares, ao que acontece nos recônditos de seu lar e até mesmo às suas características pessoais, para além de um enfoque histórico restrito à sua extensão física, afinal o resultado de um eventual ataque às aludidas projeções de sua personalidade é semelhante (senão pior) a uma agressão "simples" ao corpo: sofrimento de cunho mental, estresse, sentimento de humilhação, esses eventualmente até mais gravosos do que uma lesão física. Em patamares atuais, o "avanço" de "exploradores", ora representados por agentes econômicos com finalidades específicas (principalmente de cunho econômico/empresarial), podem se valer das informações de um indivíduo ou mesmo de sua família/grupo para indução de comportamento por distintas maneiras, abrangendo-se aí ofertas de contratos, produtos e serviços sem que seja respeitado previamente uma esfera de sua personalidade que deveria estar protegida.

Adiante, com atenção aos fundamentos do direito à privacidade, Warren e Brandeis (1890) assinalaram que as leis que usualmente punem calúnia e injúria, por se direcionarem principalmente à respeitabilidade do indivíduo perante os concidadãos e a comunidade em que vivem, normalmente guardam mais conexão com os reflexos materiais provenientes dos atos sofridos (a exemplo de maior dificuldade na interação com pessoas após um episódio de vergonha pública), do que com os imateriais.

Nesse contexto, o direito à privacidade deve ser objeto de reflexão autônoma, pois os fundamentos que geraram a compreensão acerca de sua existência hão de ser os mesmos a orientarem os problemas presentes e futuros que envolverem a proteção do indivíduo em aspectos que vão além de sua compreensão essencialmente física.

Em continuidade, afirmam que a ordem jurídica deve assegurar aos indivíduos o direito de determinar e escolher, de ordinário, qual será o alcance da extensão e transmissão de seus pensamentos, sentimentos e expressões, dosando a sua comunicação e exposição a outros conforme seu intento, não havendo de ser o cidadão compelido a agir em contrariedade a si , em proximidade ao que as leis de propriedade intelectual disciplinam. E, ademais, no caso de o indivíduo concordar com a disseminação de informação sobre si, é lícito que ele detenha o poder de fixar o limite da publicidade (o que se relaciona à denominada "autoderminação

informativa" a ser abordada), não detendo tais circunstâncias um enfoque material/retributivo ou financeiro (como um direito autoral), mas imaterial, com deferência de importância ao próprio fato de cunho privado[2] que é digno de proteção, independentemente de valores e contextos ligados ao que usualmente se denomina propriedade.

Consequentemente, características pessoais, informações do entorno e os meios de expressão, exemplificados por dados pessoais, devem ser protegidos por seu valor intrínseco ligado ao indivíduo, independentemente de seu conteúdo. Essa violação é equiparada à gravidade de uma prisão sem devido processo legal, uma acusação baseada em prova ilícita ou agressão física sem justificativa, cenários indiscutivelmente protegidos. Para salvaguardar essas manifestações, é necessário ir além das analogias usuais relacionadas à proteção contratual, real ou criminal. Reconhecer um direito autônomo, oponível a todos, com a previsão de mecanismos para responsabilização e proteção, torna-se imperativo.

A violação a uma dessas facetas da individualidade, abordada também como um ataque ao direito a ser deixado sozinho ou em paz, pode gerar sofrimento e problemas, conquanto não seja necessariamente a pessoa lesada diretamente em seu patrimônio.

Assim, havendo um princípio geral a ser invocado para tutela da privacidade, resguarda-se o indivíduo de qualquer invasão, seja pela imprensa, por um fotógrafo ou mesmo por entes que detenham dispositivos modernos aptos a captar dados (ou, atualmente, por empresas).

A propósito, é patente a necessidade de tutela de aspectos variados da personalidade passíveis de representação (a exemplo de dados expostos) por um "eixo" comum e autônomo, pois por vezes sequer há a proteção de um vínculo prévio entre os envolvidos, como um contrato, a fim de que dele se retire um regramento específico para a proteção de uma das partes lesadas por alguma sorte de ato indevido (como uma exposição, publicação ou uso indevido de informação).

Assim sendo, diante da existência de dispositivos (a exemplo dos atuais sites que cooptam dados de consumidores) que permitem acesso mais detalhado às vidas dos cidadãos, a proteção deve repousar sobre uma base mais ampla e a todos acessível e oponível, qual seja o reconhecimento da inviolabilidade da personalidade, a ser doravante denominada, acorde raciocínio de Warren e Brandeis (1890), de direito à privacidade.

Em perspectiva atual, sendo as informações de cunho pessoal (representadas em dados) relevantes para que empresas detenham material de trabalho, seja para realização de

[2] Os autores citam uma frase atribuída a "Lord Cottenham" (1820 apud WARREN, BRANDEIS, 1890, p. 10) no sentido de que "*um homem é aquilo que é exclusivamente dele*".

ofertas, para definição de nicho a ser alvo de mercado, ou para continuidade de obtenção de lucros com novos serviços, inserem-se as empresas no mesmo panorama limitador de devassa. Desse modo, havendo limitação de acesso a dados pessoais, pois por trás deles há o indivíduo a ser respeitado, é relevante ao trabalho examinar o que Warren e Brandeis estipularam como diretrizes e "remédios" (no século dezenove) ante as novas possibilidades de ofensa ao indivíduo.

Considerando as premissas por eles elencadas, ao final do estudo Warren e Brandeis (1890) fixaram seis diretrizes para definição dos limites do direito à privacidade e sua possível flexibilização ante o interesse público, com auxílio dos precedentes e análises já existentes sobre os crimes contra a honra e as leis de propriedade intelectual: i) é possível que, em acordo ao caso concreto, o direito à privacidade ceda ante o interesse público, detendo-se a proteção ao indivíduo essencialmente aos casos de exposição indesejada de sua vida privada (hábitos, atos e relações) e sem justificativa relevante; ii) inexiste violação quando a descrição de circunstância relacionada à vida privada ocorre no seio de processos ou atos relacionados a julgamentos e análises em órgãos públicos ou de interesse público, porquanto da própria natureza do ato levado a efeito; iii) reconhecimento de inexistência de danos e, consequentemente, de responsabilização, em caso de violação de privacidade sem mínima relevância ou consequência (exemplo de uma comunicação oral, e não escrita, sem repercussão ou abrangência); iv) o direito à privacidade cede ante a publicação dos fatos pelo próprio indivíduo ou com o seu consentimento; v) a verdade da exposição indevida não se configura em defesa idônea em favor do invasor, pois o foco do direito à privacidade não é a proibição de retrato impreciso da vida privada ou a defesa do caráter do indivíduo (que já tem tutela pela lei penal), mas a proibição do ataque à privacidade do indivíduo por si só; vi) e, por último, a eventual ausência de má-fé por parte do invasor igualmente não é fundamento válido para defesa, pois a lesão ocorre independentemente dos motivos de quem lesa, bastando a voluntariedade no ato.

Tais diretrizes, aliás, são coerentes com instrumentos e conceitos que atualmente são considerados pela legislação específica (LGPD), a exemplo do atendimento ao interesse público (art. 4º, § 1º), uso em processos judiciais (art. 7º, VI) e permissivo decorrente de consentimento (art. 7º, inciso I), havendo espaço para que melhor se trabalhe em âmbito regulatório a ideia do dado pessoal como verdadeira projeção do indivíduo, descurando-se por completo possível defesa por parte de um "invasor" no sentido da eventual ausência de prejuízo ao titular dos dados, ou ausência de má-fé por ocasião de meios outros como o uso de tecnologia. Em fechamento, adotando como base instrumentos correlatos a estudos

vinculados aos crimes contra a honra e aos direitos autorais, estipulam duas ferramentas a serem empreendidas como remédios jurídicos em caso de invasão de privacidade: manejo de ação para responsabilização civil por danos com o fim de se obter indenização; e busca por uma fixação judicial de obrigação de fazer ou não fazer. Há, dessa forma, espaço para debate acerca da atual suficiência ou não desses remédios para tutela de direitos de titulares de dados pessoais.

Finalizam, então, o artigo pontuando que o mesmo estado que protege a privacidade do lar perante as próprias autoridades estatais (ver limitações constitucionais ao ingresso em residência, conforme art. 5º, inciso XI, da Constituição da República) não pode, deliberadamente, permitir que se abram as portas à curiosidade excessiva ou mal intencionada, sendo necessário, portanto, o reconhecimento formal do direito de privacidade ao indivíduo.

Com atenção agora à realidade brasileira, o direito à privacidade, com suas respectivas expressões, é reconhecido desde 1988 como um direito fundamental. A Constituição Federal (CF), nesse sentido, previu em seu art. 5º, inciso X, a inviolabilidade da "intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", acolhendo-se de plano um dos possíveis remédios indicados por Warren e Brandeis (1890), o qual é a reparação em dinheiro. Previu, também, nos incisos XI e XII do mesmo artigo, a inviolabilidade da casa, das comunicações e dos dados dos indivíduos.

Nesse contexto, Tavares (2017, p. 488), citando os Estados Unidos (que na seara "direitos fundamentais" detém histórico jurídico/constitucional de realce), aponta que "a doutrina, dogmática e jurisprudência norte-americanas utilizam a referência a um direito à privacidade (*the right to privacy*) como um conceito guarda-chuva, no qual se incluem diversos direitos", todos com previsão no texto constitucional, embora em dispositivos diversos do art. 5º. O referido autor ainda aduz que o direito à privacidade acoberta os direitos à intimidade, vida privada, honra, imagem, inviolabilidade do domicílio, entre outros. Mais adiante, aproximando os conceitos de vida privada e intimidade, aponta que "a vida privada diz respeito ao modo de ser, de agir, enfim, o modo de viver de cada pessoa" (TAVARES, 2017, p. 500). Em outras palavras, tutela-se na privacidade o direito de o cidadão desenvolver sua vida em ambiente público, quando envolvido com o meio externo, e privado, na casa, com a família e em contextos de maior reserva, conforme livremente decidir. Assim sendo, por óbvio, as informações correlatas à pessoa não hão de ser registradas, indefinida e indevidamente utilizadas pela sociedade e pelo Estado:

> Tal liberdade também impede que se preservem informações obtidas referentes única e exclusivamente à privacidade de cada um, obtidas de forma lícita ou ilícita. É que não há interesse, por parte do Estado, em registrar indefinidamente a vida privada de quem quer que seja, ainda que os dados recolhidos tenham sido obtidos licitamente (TAVARES, 2017, p. 500).

Giacchetta e Meneghetti (2014), seguindo o estudo sobre a autonomia da privacidade e em desenvolvimento da reflexão sobre a natureza desse direito (em prosseguimento aos estudos clássicos), mencionam também a doutrina germânica acerca dos direitos que não seriam passíveis de serem incluídos nas espécies de direitos reais e pessoais, pois seriam ínsitos à própria personalidade, no que é denominado pelos autores de Teoria Racional ou Teoria do Direito da Individualidade. E, dentre esses direitos indissociáveis da personalidade do indivíduo, estariam, além da vida, integridade física e liberdade, a honra, segredo, identidade pessoal, resguardo, entre outros, todos inatos ao indivíduo. Ainda, refletem que a proteção da privacidade interessa não apenas ao indivíduo, embora ele seja o enfoque principal, mas igualmente à manutenção de uma estrutura social, com convivência pública e comunitária. Em desenlace, conforme recente modificação por emenda constitucional, o art. 5º, inciso LXXIX, a CF passou a prever direta a expressamente o direito "à proteção dos dados pessoais, inclusive nos meios digitais".

Enfim, o direito à privacidade, e todo o seu conteúdo histórico e normativo, é expressamente reconhecimento pelo legislador como fundamento para a proteção de dados pessoais, como se lê do artigo 2º, inciso I, LGPD, em concretização do comando protetivo genérico do indivíduo, tornando os fundamentos que alicerçam sua origem plenamente aplicáveis à proteção de dados. Se uma variada gama de opções, escolhas, características, ideologias, entre outros, podem ser consideradas projeções da personalidade e dignas da mesma atenção, os dados que as enunciam também devem ser da mesma forma protegidos em nossa realidade, e os meios aptos a causar indevida devassa a esses elementos regulados e fiscalizados.

Mais adiante, e afora a previsão normativa da proteção do indivíduo mediante a tutela dos dados de natureza pessoal, há de se pontuar que, se a tutela de dados significa em última análise a tutela do indivíduo, possui ela nítido conteúdo ético. Segundo reflexões tiradas de doutrina sobre o tema (DEZEM e DE LUCCA, 2018, pg. 12), para além dos dados que devem ser protegidos, o enfoque real se encontra nas pessoas acerca das quais os dados se referem.

Assim, embora a finalidade precípua do presente trabalho não seja o

aprofundamento das questões éticas que envolvem o tema, é inevitável tal ponderação, afinal se trata da atenção aos indivíduos e, consequentemente, do trabalho por harmônica convivência entre todos e de fixação de bons hábitos. Segundo De Lucca (2009, p. 60), "ética deriva, etimologicamente, do termo grego *ethos*, que denota o modo habitual de agir, o costume", possuindo ainda "o sentido de modo de ser ou de caráter", e uma "ciência voltada para o estudo filosófico da ação e conduta humanas" (DE LUCCA, 2009, p. 65). Em outra visão, com atenção à ética como filosofia prática, Jolivet (1959 apud DE LUCCA, 2009, p. 68) afirma que a ética "tem por fim definir o bem do homem", o que guarda ainda mais conexão com o fim último do próprio direito à privacidade, fundamento da proteção dos dados pessoais. Adiante, e com atenção ao aspecto funcional da ética e da sua consequente pertinência para elucidação dos melhores hábitos de salvaguarda do indivíduo, Cortina e Martínez (apud DE LUCCA, 2009, p. 23) entendem que a ética tem três funções, que seriam "clarificar o que é a moral e suas características específicas", "fundamentar a moralidade" e "aplicar aos diversos âmbitos da vida humana" o quanto descoberto nos pontos anteriores.

Nessa tarefa, segundo De Lucca (2009), quanto ao primeiro aspecto delineado por Cortina e Martínez, importa examinar e esclarecer o que se deve fazer e o que é possível fazer de maneira melhor do que a atual. Ainda, em tarefa de busca por fundamento das normas morais, Etxeberria (2002, p. 24) afirma que uma das funções da ética é a de "precisar igualmente os bens supremos e/ou regras, ou imperativos, que se constituem como referente moral último das nossas ações". E é essa reflexão de cunho ético (DE LUCCA, 2009) que deve proporcionar o conhecimento acerca da universalidade da normal moral, conquanto possível a existência de controvérsias. Vale dizer, o que "vale" em nosso país acorde nosso histórico e em outros, há de ser minimamente "universal" e deve referendar nossas normas de comportamento. Por tal razão é necessário que se estude, ainda que em aspecto mais restrito, a evolução do tratamento dos dados pessoais no Brasil e os apontamentos tirados por órgãos competentes em outros países sobre o mesmo tema, a fim de que daí se retirem paradigmas também éticos consoante a universalidade da norma moral (indivíduos e dados pessoais a serem tutelados em qualquer lugar), afastando-se o quanto possível o relativismo. Por último, dos exames à prática ou da vida moral à moral prática (vivência), é devido que se traduza em vivência moral o quanto foi refletido em cunho ético, no que se pode denominar de ética aplicada (DE LUCCA, 2009), tendo como exemplos a bioética e a ética empresarial. E, no que toca à ética empresarial, para fins deste estudo, após exame de histórico de gestão de dados no Brasil e de decisões em outros países, projeta-se a estruturação de um mínimo de diretrizes a serem seguidas por empresas e empresários com fins de conformidade à

privacidade dos indivíduos e de seus dados pessoais, à luz do que o novo diploma (LGPD e seus fundamentos) apresenta, para melhor atuação em sociedade.

1.3 A proteção de dados no Brasil até o advento da Lei Geral de Proteção de Dados Pessoais

Antes que se examine a LGPD em si, é necessário que se reflita sobre o percurso vivenciado no Brasil até o seu advento, afinal, muito embora se estude o direito de privacidade há séculos, a lei pátria sobre dados pessoais é de 2018, e seu surgimento derivou de demandas específicas. Aliás, tal apuração permitirá a ponderação sobre o patamar protetivo em que efetivamente nos encontramos sob determinado recorte (especialmente no que toca ao tratamento de dados de cidadãos por empresas e a litigiosidade decorrente dessa relação), valendo-se para tanto da comparação entre algumas das ferramentas e problemas que atualmente são utilizados e vivenciados e as diretrizes derivadas dos mesmos instrumentos que poderiam ser utilizados de forma mais eficiente, acorde nosso atual estágio de compreensão do direito à privacidade e proteção de dados.

Nessa incumbência, verifica-se que décadas após a previsão de proteção constitucional da intimidade, da vida privada, das comunicações e dados, em 2011 foi aprovada a lei 12.527/2011, denominada Lei de Acesso à Informação (LAI), que "regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal".

Segundo Doneda (2021b), em um primeiro momento histórico foi o Estado quem se encontrou na posição de se utilizar das informações pessoais de forma mais intensa (a exemplo de coleta de dados por meio de censo), afinal, mediante maior conhecimento da população, amplificam-se as possibilidades de uma administração mais eficiente.

Ainda, de início, era o Estado quem dispunha de meios mais eficazes de obtenção de dados, sem que igual disponibilidade de meios e de custos fosse permitida aos entes privados. Apenas com o desenvolvimento de tecnologias que facilitavam a coleta e processamento de dados pessoais é que a atividade passou a ser atraente também para organismos da iniciativa privada (DONEDA, 2021b). Natural, portanto, que a Lei de Acesso à Informação fosse elaborada em instante anterior à LGPD, afinal em origem foi o ente público o principal coletor de informes de cunho pessoal, sendo ele então o destinatário de deveres como a transparência. Inaugura-se, dessa forma, uma maneira específica de manejo das informações públicas em reconhecimento de um direito fundamental do cidadão de acessar as informações detidas pelo Estado, tornando governos aptos a serem fiscalizados e criticados (MICHENER;

CONTRERAS; NISKIER, 2018).

Em observação específica, dispõe a referida lei em seu art. 1º estatuídos ali os procedimentos a serem observados pelos entes federativos a fim de se garantir o acesso a informações pelo cidadão, garantindo-se um "direito fundamental de acesso à informação" (art. 3º). Dentre as diretrizes a serem adotadas nesses procedimentos, encontram-se a adoção da publicidade como regra e o sigilo como exceção, divulgação de informações de interesse público independente de solicitações e fomento à transparência na administração pública (art. 3º). Ainda, o art. 4º, inciso I, LAI, em relevante previsão, conceitua informação como dados, processados ou não, que podem ser utilizados para transmissão de conhecimento.

Em sequência, a referida Lei permite classificação das informações, acorde sua relevância para salvaguarda da segurança da sociedade ou do Estado, em ultrassecretas, secretas e reservadas, com distintos prazos de restrição (arts. 23 e seguintes).

Em estudo específico e acorde os dispositivos da Lei em comento, Gruman (2012) distingue os deveres da Administração, quanto ao manejo das informações, em "transparência ativa", quando há dever de divulgação de informações de interesse coletivo e do cidadão por parte do Estado mediante iniciativa própria (arts. 7º e 8º), mormente quando relacionadas a programas, projetos, ações do governo e metas, e "transparência passiva", oportunidade no qual o ente público deve divulgar mediante atendimento às solicitações provenientes da sociedade. Semelhantes raciocínios são também apresentados por Jardim (2012), ao apontar que as noções de transparência ativa e passiva são igualmente implementadas em outros países, e prevê a necessidade de que o Estado se antecipe, no que toca à transparência em sua vertente ativa, na transmissão de informações que sejam realmente úteis ao cidadão, antes mesmo dos pedidos a serem requeridos em contexto de transparência passiva.

Ainda, contextualiza Gruman (2012) que mediante a inovação legislativa o Estado passou de um garantidor de sigilo das informações (em panorama relacionado à ditadura militar) para um garantidor de estabelecimento de mecanismos de acesso à informação pública. Com o advento da LAI, o sigilo se torna a exceção e a publicidade a regra, em maior cuidado com informações a serem repassadas aos indivíduos, com vistas à consolidação da transparência e democracia, afinal a possibilidade de influência dos indivíduos na tomada de decisões se fortalece. Em sequência ao estudo, apresenta conceitos de assimetria, simetria e democracia.

Nessa reflexão, disserta que temas e debates existentes em uma determinada sociedade passam a se tornar efetivamente públicos quando são admitidos e adentram em espaços abertos à coletividade, mencionando como *locus* as ruas, praças e instituições (a exemplo de temas

religiosos, de orientação sexual, proteção a vulneráveis , corrupção, entre outros).

Para tratamento e debate desses temas são criadas as políticas públicas, existentes para se prestar atenção às decisões e entendimentos fixados durante as reflexões nos espaços públicos. Diferentes pautas são aptas a ingressar em espaços dessa gama acorde reivindicações da sociedade civil, movimentos sociais, representantes governamentais, entre outros. Assim sendo, o poderio de determinado grupo ou indivíduo pode condicionar a tomada de uma decisão, ou fixação de um entendimento, em detrimento de outros grupos. Assimetria, então, mostra-se como uma anomalia de poder entre Administração e administrado, em razão do monopólio de informações detidas pelo primeiro. Simetria, ao seu turno e nesse mesmo panorama, indica maior similitude de poder de influência em razão de os governandos também deterem informações e, consequentemente, maior força para influência em decisões. Gruman (2012) encerra o raciocínio pontuando que "informação é poder" e, via de consequência, em uma sociedade verdadeiramente democrática haverá livre fluxo de ideias e interpretações, pois os cidadãos terão maior conhecimento e maior capacidade de convencimento em razão da garantia do direito fundamental à informação (se possuem os dados, possuem o conhecimento). Ser cidadão, dessa maneira, não significa apenas exercer voto, mas também exercer contínua influência nos rumos a serem tomados por ocasião do respeito aos seus direitos.

Neste quadro, em um primeiro momento o próprio Estado atuou como um detentor de informação que declara ciência sobre o poderio do manejo de dados. E estatuiu ferramentas e diretrizes direcionadas à equalização de assimetrias, permitindo que entes públicos e cidadãos usem as informações provenientes de dados para fins úteis e coletivos. A partir de então, se respeitado o histórico legislativo no trato com dados, é possível refletir que os dados e as informações deles extraídas não devem ser concentrados em um ente único e, menos ainda, serem utilizados sem transparência, valendo o mesmo, no que for compatível, como guia indicativo para relações entre empresas e cidadãos.

Os autores Michener, Contreras e Niskier (2018), ao avaliar a LAI cinco anos após a sua vigência, apontam que em realidade o Estado passou de um depositário de informações públicas para um gestor, ressaltando uma vez mais o reconhecimento pelo legislador brasileiro de que "informação é poder".

No mesmo trabalho indicam possibilidades de incremento na eficiência da lei, tais quais melhoria no tratamento da transparência passiva (que demanda resposta a requerimentos), vez que a transparência ativa (dever de informar sem provocação anterior) permite uma "higienização" do conteúdo a ser informado, além incremento de métodos de supervisão e

execução independentes e não sujeitos à autoridade responsável pelos dados. Ainda, acorde pesquisa desenvolvida à época do artigo, apontam que o maior déficit de resposta aos pleitos de informação, com menor regulamentação e execução, ocorre em âmbito municipal, justamente a esfera mais próxima dos governados, e que a existência de plataformas digitais oficiais ou canais online específicos para atendimento de demanda de informações influenciam de forma decisiva a transparência do ente governamental, possibilitando melhor acesso aos cidadãos. Nesse mesmo sentido pontua Jardim (2012), ao mencionar na época que, apesar de ser um órgão relevante na estrutura do Executivo Federal e com papel de atuação em serviços de informação, a Controladoria Geral da União (CGU) não é uma agência especializada em gestão da informação governamental, mencionando ainda a pluralidade na definição de agências responsáveis pela lei de informações em âmbito estadual, sem o caráter de maior uniformidade ora melhor trabalhado pela LGPD (a exemplo da fixação de autoridade nacional para proteção de dados). Em arremate, Jardim (2012) afirma que o descompasso entre o cidadão "epicentro numa ordenação jurídica" e a efetiva ordenação no plano informacional há de ser progressivamente diminuída, com melhores condições reais de acesso à informação.

Afinal, as maneiras pelas quais ocorre a produção, transmissão e uso das informações/dados são capazes de apresentar uma espécie de face ao cidadão, em benefício de um regime mais democrático à medida que se torne menos opaco o Estado.

Em finalização ao estudo da Lei de Acesso à Informação, tem-se que o referido diploma de 2011 tratou, em um primeiro plano de dados manejados pelo Poder Público (não de forma direta dos dados de cunho pessoal), em uma relação verticalizada entre cidadão/Estado, mas reconheceu patentemente o poderio gerado em razão do conhecimento que as informações conseguem ensejar aos seus detentores, estabelecendo forma de gestão para acesso, na finalidade também de promoção de equilíbrio e justiça na sociedade.

Ainda com atenção aos objetivos do estudo, de rigor o exame do Marco Civil da Internet, que pavimentou o trajeto para o posterior advento da LGPD. Segundo Teffé e Moares (2017), as relações interpessoais e a exteriorização da vontade humana são propagadas pelos mais diversos atos aptos a serem exteriorizados em sociedade, traduzindo-se tais expressões pela busca por interesses subjetivos e sociais. Certo é que, com esse escopo, a internet e seu específico método de manejo de dados se revelou um mecanismo essencial para a adaptação humana em mundo que, de fato, é eivado de tecnologia e de significativa movimentação de capitais.

Em aspecto adicional, a natureza global da internet e a inexistência de um regulador centralizado para disciplina das ações desenvolvidas nesse meio impôs a necessidade de

estudos e reflexões acerca de suas consequências para a vida dos cidadãos. E, nesse contexto, é que surge a lei 12.965 de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, e basicamente confere estrutura fundamental às relações jurídicas em curso nos ambientes de tecnologia, acorde Leite e Lemos (2014), sendo ela apelidada de "Constituição da Internet".

Os autores, em obra conjunta com outros, apontam que um dos relevantes motivos para a existência de uma legislação considerada como "marco" para as relações em redes virtuais, para além da globalização econômica e financeira, comércio internacional, entre outros, é a exigência de neutralidade.

Vale dizer, considerada a internet como uma rede "fim a fim" (GETSCHRO; 2014, p. 13), há de se garantir que inexista indevida interferência na transmissão de dados entre uma extremidade da comunicação e outra (afinal a mensagem necessita ser repassada), tal como em outros sistemas tradicionais de transmissão de mensagens, sem violação de sigilo e em uma sociedade interligada e informacional. A propósito, uma das disposições constantes do "Marco Civil da Internet" é precisamente a ausência, em regra, de responsabilidade do provedor de internet pelos conteúdos produzidos por terceiros (art. 18), haja vista o dever de neutralidade.

Mais adiante, pontua Lima (2014) que os usuários e suas condutas são, ainda que em ambiente neutro e virtual, passíveis de serem identificados por protocolos específicos, como o IP *(internet protocol*), gerando a necessidade de se proteger, além da neutralidade das comunicações, a privacidade dos cidadãos e de seus dados, e de se refletir sobre até que ponto tais informações podem ser acessadas por terceiros (dentre instituições privadas, como bancos, e públicas, como órgãos de investigação), a depender do contexto.

Teffé e Moraes (2017), no mesmo entendimento, apontam que o princípio da neutralidade da rede disserta sobre o direito ao tratamento igualitário dos dados informativos dos envolvidos na comunicação, sem distinção do conteúdo de transporte e sem discriminação do usuário, albergando a liberdade de expressão, sem se descurar, em outro vértice, do princípio da privacidade, que visa a circulação segura das informações pessoais. Ambos, transmissão da mensagem e dos dados e proteção da mesma mensagem e dos dados são valores de relevo. E, nesse preciso contexto de conferência de valor não só à mensagem, mas também ao mensageiro, o art. 3º da referida lei, que é anterior à LGPD, indica como princípios fundamentais que disciplinam o uso da internet a proteção da privacidade e dos dados pessoais, nos incisos II e III. Ainda, no art. 7º garante ao usuário o sigilo do fluxo de suas informações pela internet e de informações armazenadas e de cunho privado; bem como devido

esclarecimento acerca do uso, armazenamento, tratamento e proteção de seus dados pessoais, que só poderão ser utilizados para finalidades específicas justificáveis, lícitas e relacionadas ao serviço contratado (incisos II, III e VIII).

Os incisos IX e X, por sua vez, asseguram que o tratamento dos dados de um usuário deverá ser precedido de consentimento expresso e em cláusula separada, e exclusão dos dados coletados mediante requerimento ou na hipótese de encerramento da relação (essa última garantia adicionada pela Lei Geral de Proteção de Dados). Todas essas conquistas fixadas pelo legislador, posteriormente, foram mais detalhadas na LGPD, com acréscimo das previsões das hipóteses específicas de tratamento de dados, responsáveis pelo manuseio e cuidado das informações, maior detalhamento das condições de consentimento, direitos específicos do titular de dados, distinção entre espécies de dados (sensíveis ou não), entre outros.

Em continuidade dos estudos acerca do Marco Civil da Internet, Lima (2014), em artigo publicado antes mesmo da vigência da LGPD, conceituou "dados" como:

> [...] qualquer informação que permita a identificação, direta ou indireta, de um usuário, incluindo dados cadastrais (nome, filiação, endereço, documento de identificação e e-mail, por exemplo) e técnicas (endereço de IP), sem prejuízo de conter também referências cujo tratamento pode representar discriminação do usuário (dados biométricos, de raça, saúde, entre outros) (LIMA; 2014, p. 155).

Lourenço e Guedes (2014) também apresentam diferenças entre dados e informações. Acorde suas reflexões, dissertam que dado é uma espécie de elemento quantificável e, de certa forma, "puro", acerca de algo. Já a informação conteria um elemento valorativo, e seria a análise do dado seguida da ocorrência de um determinado conhecimento. Assim, a ordenação ou concatenação de dados pode, ou não, produzir uma informação. Em exemplo, o acesso a registros de compras (dados) de determinado cidadão pode levar ao conhecimento de seu perfil, preferências e condições econômicas (informações), quando então poderão tais dados serem considerados de cunho pessoal.

Teffé e Moraes (2017), em comentários aos aplicativos de redes sociais, apontam que o fornecimento de dados pelo próprio usuário se dá por vezes de forma até não consciente, com crescente aumento de coleta indiscriminada por empresas envolvidas com o ambiente virtual. E, se considerados tais mantenedores de dados como não dotados de substancial controle, torna-se possível, por intermédio da arregimentação de informações, a delimitação de padrões de comportamento de cada usuário, com elaboração de perfis de consumo e conhecimento de patrimônio pessoal.

Diante dessas disposições, apontam que os registros eletrônicos e as informações que permitam identificar o cidadão-usuário apenas poderão, em regra, ser disponibilizadas pelos detentores em razão de pleito de autoridades competentes, nos termos do art. 10, § 3º.

Em seguimento, o fornecimento de dados coletados em ambiente digital a terceiros, fora as autoridades, apenas poderá deter ensejo em caso de consentimento do usuário, conforme o art. 7º, IX. O enfoque de toda essa proteção é, ao final, a segurança do indivíduo que utiliza a internet, que deverá permanecer consciente da coleta e da finalidade do tratamento de seus dados, e até mesmo da segurança e cuidado existente sobre essas informações pessoais, em exercício da liberdade que a rede proporciona. Em problematização e no âmbito privado, os autores (LIMA, 2014) até admitem a fiscalização das atividades de funcionários pelos empregadores, desde que a rede utilizada seja corporativa, ou seja, vinculada às próprias atividades da empresa, com respeito às legislações pertinentes (como a trabalhista), e desde que os trabalhadores sejam previamente informados disso, com cientificação deles de que a privacidade se encontra justificada e pontualmente restringida. Todavia, em regra e conforme o art. 7º, VII, o usuário de internet tem o direito de ser protegido quanto às indevidas transmissões ou monitoramentos de seus dados pessoais, sendo abarcadas aí a tutela de seus registros de conexão e acesso de aplicações de internet.

Vale dizer, ainda que a Lei do Marco Civil da Internet não tenha como fulcro específico a tutela de dados, mas sim das comunicações efetuadas pela internet, foi um diploma que surgiu anteriormente à LGPD haja vista que a tecnologia em si avança em patamar mais rápido do que as reflexões jurídicas sobre os resultados de seu avanço (dentre eles a maior exposição de dados), assim como afirmaram Warren e Brandeis (1890). Ainda assim, há de se pontuar que a própria lei reguladora em primeiro plano das relações empreendidas via internet apresenta um indicativo mínimo da necessidade de proteção de dados, a indicar que a tecnologia e as possibilidades por ela geradas devem respeitar o indivíduo, garantindo-se que nada, nem mesmo ambientes virtuais, escape de um viés valorativo em favor dos direitos das pessoas envolvidas.

Em sequência, Lima (2014) aponta que os provedores de conexão devem resguardar o sigilo de informações como duração do acesso à internet e endereço de IP. Para tanto, o art. 5º, em seus incisos VI e VII, conceitua registros de conexão como “o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”, e registros de acesso a aplicações de internet como “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”. Enfim,

é nítido que tal gama de informações e rastros deixados na internet pelo cidadão detém limitações de uso e monetização pelos portadores em benefício de uma maior autodeterminação por parte dos usuários. Em último apontamento neste tópico, Giacchetta e Meneghetti (2014) apontaram (à época da confecção do estudo, considerando que a obra consultada é anterior à vigência da LGPD) que o Marco Civil da Internet, conquanto dotado de disposições acerca de proteção de dados e privacidade, dissertou acerca do tema de forma ainda imprecisa e incompleta, sem delimitar atividades e ações ou estruturar um mínimo de capacidade regulatória nessa seara, a evitar ou minorar os efeitos de coletas de dados sem consentimento, ou sem consentimento esclarecido (citam o caso do aplicativo "Google Street View" e questionamentos sobre usos dos dados coletados pela empresa, aplicativos que permitem localização dos celulares, entre outros). Ao final, explicitam que o diploma legislativo da internet sequer enuncia um conceito de dados pessoais ou disciplina o específico tratamento de dados sensíveis, e indicam também que uma possível lei de dados (ora já existente e vigente) deve contemplar o devido cotejo entre tratamento de dados, proteção de dados e privacidade.

Enfim, o Marco Civil da Internet se direcionou primordialmente à regulação da transmissão de informações em si, em um viés "objetivo" da comunicação via internet, com atenção à segurança e neutralidade. Por óbvio tal necessidade é patente, afinal as comunicações por internet são realidade inconteste e inafastável do convívio em sociedade, havendo de se considerar a importância de relações que, graças à tecnologia, são horizontais (usuários privados de internet), ao contrário do objeto da Lei de Acesso à Informação, que trata da relação verticalizada entre cidadão e Poder Público. No entanto, o Marco Civil somente tangenciou em 2014 a proteção ao indivíduo ao enunciar princípios específicos como proteção de dados e privacidade, e apresentou o consentimento como uma baliza para determinadas hipóteses de uso de dados pessoais, não direcionando dessa forma suas atenções principais ao usuário e suas informações, mas à comunicação.

Em cotejo com os objetivos deste trabalho, o acesso a informações das pessoas por empresas e a comunicação com elas por diversos meios, principalmente a internet, tornou-se fenômeno, de fato, patente, eficaz, regulado e participante dos diversos cenários de contratação. E o Marco Civil consagra a tecnologia como um dos principais, se não o principal, meio de contato entre empresários/empresas e clientes (no mínimo entre provedores de acesso e usuários de internet). Ainda assim, não é o suficiente. Há de se perquirir sobre a forma de obtenção dos dados que permitem essa comunicação, bem como sobre os usos que deles serão feitos, e todo esse cenário conjugado com a participação e consentimento do titular. Além de

se vedar a assimetria de informações (que já é um dos objetos da LAI) e de se garantir a neutralidade e eficiência das comunicações (enfoque do Marco Civil), há de se tutelar o mensageiro que, por detrás de todas as tecnologias é um cidadão dotado de direitos.

Em síntese, reguladas as transmissões de dados por meio da internet, restou aberto o caminho para, anos após, a implementação de um diploma que, por sua vez, considerasse a regulação do tratamento de dados por si só (considerando o indivíduo a eles relacionado). O próprio contexto existente com o desenvolvimento da tecnologia e da internet leva à indissociável necessidade de análise da proteção autônoma de dados e informações pessoais, à luz do direito à privacidade, afinal a posse de informações por pessoas e empresas com o desenvolvimento da tecnologia altera efetivamente o "eixo" de poder, antes exercido eminentemente pelo Estado e suas possibilidades de coleta e uso (DONEDA, 2021b). Antes os próprios entes públicos se preocuparam (estabelecendo a Lei de Acesso à Informação) com a possível assimetria gerada pelo seu concentrado controle de dados, e agora há de se atentar igualmente à possível assimetria gerada por empresas que guardam grande potencial de aquisição e manejo de dados pessoais.

Pontua nesse sentido o autor:

> [...] o controle sobre a informação foi sempre um elemento essencial na definição de poderes dentro de uma sociedade, a tecnologia operou a intensificação dos fluxos de informação e, consequentemente, de suas fontes e seus destinatários. Essa mudança, a princípio quantitativa, acaba por influir qualitativamente, mudando a natureza e o eixo de equilíbrio na equação entre poder – informação – pessoa – controle. Isso implica a necessidade de conhecer a nova estrutura de poder vinculada a essa nova arquitetura informacional. (DONEDA, 2021b, p. 35).

Nessa toada, é adequado então o estudo da LGPD, promulgada em 14 de agosto de 2018, e de seus fundamentos. A LGPD, em patamar mais amplo e detalhado do que o feito por leis anteriores, dispõe acerca do tratamento de dados pessoais nos setores público e privado, para proteger direitos fundamentais como o da privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural, e é "inspirada em parâmetros internacionais, em especial, nos parâmetros estabelecidos no Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection – 'GDPR')" (COELHO; LOTUFO, 2019, p. 226-227).

É, assim, aplicável a qualquer pessoa natural ou jurídica que realiza tratamento de dados pessoais, independentemente do meio (ainda que fora do contexto da internet).

Doneda (2021a) reflete que a proteção de dados pessoais tem suas origens no direito à

privacidade e, de forma mais ampla, no fortalecimento de direitos individuais.

Adiante, pontua que em um determinado instante histórico, com um processamento automatizado dos dados pessoais, houve de se estudar de forma mais acurada a proteção dos cidadãos diante dos riscos surgidos, com conferência de mais autonomia à específica disciplina dos dados pessoais.

O aumento do tratamento dos dados, sua complexidade e intensidade de transmissão e gestão geraram necessidade de também maior estudo da disciplina, com inclusão de caracteres antes não estipulados, incluindo-se aí legislação e regulação sobre o tema.

Nesse panorama, o cotejo entre liberdade da expressão, segurança das comunicações, segurança jurídica dos mercados e proteção de dados são desafios enfrentados por todos os países. Assim sendo, e a par dos diplomas esparsos surgidos no continente europeu e do estudo de Warren e Brandeis (1890), Doneda (2021a) aponta a realização do censo alemão de 1982 como um relevante marco da proteção dos dados pessoais (conquanto o desenvolvimento do tema tenha sido lento, a considerar a aprovação da lei europeia de dados, a GDPR, apenas em 2016).

A corte constitucional da Alemanha, ao considerar o significativo volume de processamento de dados decorrente do avanço da tecnologia, terminou por reconhecer o princípio da autodeterminação informacional, derivado dos direitos da personalidade, e direcionado ao controle e regulação da abrangência da divulgação ou uso dos dados coletados. Via de consequência, deve-se resguardar ao indivíduo um mínimo de controle das suas próprias informações, sem que se considere o titular como apenas mais um dado em si, e sem qualquer chance de influência ou participação. Segundo os autores, a Corte assim pontuou:

> Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (dados relativos à pessoa [cf. § 2 I BDSG – Lei Federal sobre a Proteção de Dados Pessoais]) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. (BIONI, 2021, pg. 28).

Tal raciocínio garante, segundo as reflexões dos estudiosos, maior centralidade do indivíduo no controle dos seus dados, afinal todos eles têm a sua importância e valor. Teixeira e Guerreiro (2022, p. 13) bem explicam o conteúdo da autodeterminação informativa: “poder que o indivíduo tem de determinar como seus dados serão tratados mediante o recebimento de

informações sobre como será esse tratamento". O cidadão, assim, tem o direito de saber quais dados pessoais estão sendo coletados e tratados, quando ocorreu tratamento e qual a finalidade dele.

Assim, com maior conhecimento do manejo de seus dados por terceiros, tem ele informações suficientes para determinar se aquiesce ou não com aquela prática, garantindo-se a ele maior controle. Tal preocupação é plenamente justificável, pois ainda que a princípio um dado possa não oferecer uma informação de relevo sobre uma pessoa, se analisado conjuntamente a outros, cruzado, transferido ou organizado, pode levar a informações precisas ou sensíveis sobre alguém (BIONI, 2021).

Nesse raciocínio, o conceito de dados pessoais previsto na LGPD, art. 5º, inciso I, é genérico, e delega aos aplicadores o encontro das informações que sejam projeções do cidadão: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

O professor Ingo Wolfgand Sarlet (2021), em estudo sobre os fundamentos constitucionais da proteção de dados, enumera a versada tutela como direito fundamental, em especial considerando o contexto da sociedade tecnológica, com incremento do uso da informática e de digitalização.

Os avanços notabilizados que influenciam todos os ambientes de convivência (âmbito social, cultural, econômico) geram maior dinamicidade e complexidade às relações entabuladas e aos dados e informações nelas contidos.

O Direito, nesse panorama, não há de permanecer indiferente, afinal, sempre há de proteger direitos humanos e individuais eventualmente atingidos, dotando o cidadão, claro, de instrumentos que lhe permitam maior controle e proteção. O autor chega a falar em "digitalização de direitos fundamentais" ou "dimensão digital dos direitos fundamentais":

> O avanço da digitalização (que, todavia, não se restringe ao problema da proteção de dados, como sabido), de certo modo, tem impactado não apenas o direito positivo, ou seja, a produção legislativa e normativa em geral, mas também 'contaminado' a dogmática e a metodologia jurídicas, além de estender os seus tentáculos para os domínios da administração pública e labor dos Tribunais, os quais, cada vez mais, são compelidos a achar soluções criativas e suficientes para dar conta dos problemas concretos que lhes são submetidos. Assim, não é à toa que já há tempos se fala em um processo de digitalização dos direitos fundamentais (ou de uma dimensão digital dos direitos fundamentais), bem como de uma digitalização do próprio Direito (daí se falar também de um Direito Digital), o que, à evidência, inclui – mas de longe não só isso! – o reconhecimento gradual, na esfera constitucional e no âmbito do direito internacional, de um direito humano e fundamental à proteção de dados, assim como de outros princípios, direitos (e deveres) conexos, mas também de uma releitura de direitos fundamentais 'clássicos' (SARLET, 2021, p. 40).

Dadas as características da prestação de serviços nos ambientes digitais, não é incomum que dados pessoais permaneçam em bancos de dados também informatizados. Assim, eventual falta de proteção ou facilidade de acesso a essas fontes de dados pode potencializar lesões a direitos, pois os detentores podem adquirir conhecimento e gestão sobre informações acerca de variados matizes sobre os cidadãos titulares. Um exemplo são os possíveis incômodos a serem gerados aos cidadãos mediante ligações em seus aparelhos, ou mesmo a oferta de serviços a pessoas de maior vulnerabilidade (a exemplo de idosos), valendo-se de suas informações (aposentados, pensionistas, entre outros) para oferta de serviços mal compreendidos por eles, com vistas à obtenção de lucros.

Muito embora o direito à proteção de dados detenha caráter fundamental autônomo, tem ele relação com outros direitos e princípios igualmente de âmbito constitucional, a impactar distintas áreas e a permitir mais acurada análise do âmbito e da efetividade da proteção. Em âmbito de maior concretude, a União Europeia promulgou o regulamento 2016/679, o denominado GDPR (General Data Protection Regulation), com eficácia a partir de maio de 2018, e que conferiu maior unicidade quanto ao tratamento dos dados em ambiente europeu. Segundo Teixeira e Guerreiro (2022, p. 9), a legislação europeia se aplica "imediatamente a todos os países da União Europeia sem a necessidade de adequações legislativas internas, um fator de extrema relevância, até mesmo em vista do fluxo de dados, que não se limita a qualquer fronteira", tornando viável a possibilidade de todos os países envolvidos gozarem da mesma proteção e segurança derivada desse instrumento. Os autores ainda pontuam que a lei do continente europeu abordou questões fundamentais sobre a privacidade em um cenário de intensa transferência de dados, incrementando também o impulsionamento de atividades econômicas vinculadas ao mundo digital, tornando então quase que inevitável que sistemática semelhante fosse gerada também no Brasil, facilitando-se as operações comerciais realizadas. Um dos fenômenos dignos de atenção da GDPR foi precisamente a regulamentação da transferência internacional de dados, o que possibilitou um maior fluxo de informações em ambiente de tecnologia e à luz de legislação harmônica (ao menos entre os europeus), o que tornou inexorável a edição de uma lei em similares moldes no Brasil, sob pena de não adequação à realidade internacional. Segundo Araujo e Danese (2020, p. 449), "o advento da GPDR (...) colocou a proteção de dados no cotidiano jurídico, além de haver pressionado o Brasil e os demais Estados que não tinham legislação sobre o tema a legislar".

Em estudo à legislação pátria, Teixeira e Guerreiro (2022), em comentários ao art. 1º da LGPD, assinalam que, na era do "big data" (termo usualmente relacionado a vultosos volumes

de dados armazenados e processados), não se encontra o Brasil a par da necessidade de se equilibrar a privacidade das pessoas com a livre iniciativa, produzindo-se regras claras sobre tratamentos de dados à sociedade:

> "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (art. 1º, lei 13.709/18).

E é atento a esse contexto de cotejo entre direitos e valores, inspirados em legislação alienígena mas também na Constituição Federal, que o legislador estipulou no art. 2º que os fundamentos da proteção de dados pessoais são: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Vale dizer, a necessidade de proteção de dados, da privacidade dos cidadãos, da intimidade, dos direitos consumeritas, entre outros, no cenário da sociedade tecnológica informacional, não exclui o dever da sociedade e das autoridades de se atentar também para valores como desenvolvimento tecnológico, livre iniciativa e livre concorrência, todos como diretrizes aos aplicadores.

Em delimitação da aplicabilidade da lei, o art. 5º aponta variados conceitos de institutos ali trabalhados. Nesse sentido, no inciso I "dado pessoal" é considerado como "informação relacionada a pessoa natural identificada ou identificável", ou seja, não apenas o dado "direto", a exemplo de um documento pessoal, é objeto de tutela, mas outros indiretos, como uma localização, é passível de gerar individualização e, consequentemente, é dado protegido, pois pessoal (TEIXEIRA e GUERREIRO, 2022). "Dado pessoal sensível", por sua vez, é classificado como "dado pessoal 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", com exigência de maior detalhamento para seu tratamento.

Em exemplo, um dado pessoal que indique a característica de aposentado, portador de problema de saúde, ideais de cunho político, e outros, deve ser questionada para propósitos específicos e de forma ainda mais transparente do que um dado que revele "apenas" a

identidade. “Tratamento”, por sua vez, é tido como operação empreendida com dados pessoais, abrangendo-se, dentre outros, “a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” dos dados.

1.3.1 Requisitos para tratamento dos dados pessoais.

Os dados pessoais, em paralelo com os estudos que deram origem ao direito à privacidade, devem ser examinados como uma projeção da própria personalidade do cidadão, afinal, a depender das informações, é possível que se identifique tanto a pessoa em si (nome, residência, entre outros) como os seus hábitos e características. O tema de proteção dos dados se torna ainda mais relevante se considerado que grandes empresas, aí consideradas principalmente as empresas de tecnologia vinculadas à comunicação e de serviços bancários, são aptas a granjear quantidade significativa de dados das pessoas, com a consequente possibilidade de influenciar comportamentos e ampliar os seus resultados empresariais, oferecendo e vendendo produtos e serviços em patamares sem aparente limitação. Nesse contexto, os dados se tornam verdadeiros “ativos financeiros” (LIMA, 2020, pg. 24), em uma espécie de competição sobre a posse de tais informações com o possível objetivo de aumentar, claro, os lucros. E é também em razão de todo esse panorama que a LGPD surge, em momento seguinte ao surgimento do Regulamento Geral sobre a Proteção de Dados na Europa (2016; com sigla em inglês “GDPR”), estatuindo requisitos para o tratamento de dados dos cidadãos e inaugurando de forma direta a regulação do tratamento de dados por terceiros no país.

O art. 7º da LGPD, nesse cenário, prevê as hipóteses que permitem o tratamento dos dados pessoais. São elas: o consentimento fornecido pelo titular (já adiantado pelo Marco Civil); o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais e quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Até aqui (advento da LGPD), tornaram-se mais delimitadas e claras as hipóteses em que

os dados podem ser requisitados e usados. De plano, verifica-se que a hipótese permissiva de tratamento por excelência é o consentimento (previsto já no primeiro inciso), em nítida atenção à autodeterminação informativa. Além disso, é permitido que se requisitem dados quando eles forem necessários à execução de um contrato. Vale dizer, em caso de requisição de um empréstimo, é lícito que se requisitem dados bancários do requerente, a fim de que a prestação (transferência do dinheiro) seja possível. No entanto, caso a finalidade seja distinta, a envolver algo como a oferta de futuros produtos ou possibilidades, haverá de existir o consentimento.

O mesmo artigo apresenta como hipóteses para legítimo tratamento a coleta de dados que sejam necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); a proteção da vida ou da incolumidade física do titular ou de terceiro; a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; 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; e a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Prevê assim a lei casos específicos em que é razoável (e mesmo necessário) que se colham dados, a exemplo da verificação de histórico de dívidas para avaliação do custo de uma operação financeira, ou dados relativos à saúde no caso de um produto, ou serviço com restrições. Enfim, conquanto extensas as hipóteses, para fins de delimentação do estudo abordaremos em prevalência o quanto relacionado aos incisos I (consentimento), II (cumprimento de obrigação legal ou regulatória), V (necessidade para execução de contrato) e IX (proteção de interesses legítimos do controlador).

O consentimento é a primeira, se não a principal, hipótese de tratamento de dados. A referida condição detém tanta posição de relevo que inaugura as hipóteses permissivas de tratamento, conforme prevê o art. 7, inciso I, LGPD, assegurando assim a lei maior participação do indivíduo no fluxo de suas próprias informações, segundo estudos de Viola e Teffé (2021).

Além disso, prevê o art. 5º, inciso XII, da LGPD, que o consentimento, para fins da lei específica, é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". "Livre" tem o sentido de permissão ao titular de escolha sem intervenções ou situações que viciem seu consentimento. "Informado" significa a compreensão da maneira pela qual os seus dados

serão utilizados. “Inequívoca”, por fim, guarda o sentido de ausência de obscuridade, ou seja, o consentimento fornecido com a clara noção do que se pratica, por parte do titular (VIOLA e TEFFÉ, 2021).

O legislador guardou, nesse panorama, a preocupação de explicar por vias expressas o que significa um consentimento substancialmente válido, e não apenas formalmente válido. Uma coleta de dados requisitada condicionadamente à obtenção de alguma informação devida, atualização de softwares ou aplicativos, ou mesmo descontos no serviço oferecido pode não significar um consentimento verdadeiramente livre. Uma “confirmação” de dados pessoais por telefone, sem real explicação do porquê da importância de aqueles dados estarem corretos (na hipótese de abordagem feita por empresas), pode não significar um consentimento de fato “informado”.

De plano, demonstra a LGPD preocupação no sentido de que o consentimento seja o menos “manipulado” o possível, mormente quando os usuários apresentem alguma vulnerabilidade (a exemplo de idade ou enfermidade).

Nesse raciocínio, segundo a mesma doutrina (VIOLA e TEFFÉ, 2021), há destaque nos dispositivos para a atenção do legislador no que toca à concretização, orientação e reforço do controle dos dados por meio do consentimento qualificado pelos moldes legais. Acorde leitura dos dispositivos da LGPD, o consentimento, dentre outros, deve ser escrito em cláusula destacada ou fornecido por meio que demonstre a manifestação de vontade (art. 8º), obtido sem vício de consentimento (art. 8º, § 3º) e dotado de finalidades determinadas e não genéricas (sob pena de nulidade; art. 8º, § 4º).

O consentimento também é nulo caso as informações fornecidas ao titular tenham conteúdo abusivo (art. 9º, § 1º). De plano, tomadas essas premissas, infere-se que, segundo a LGPD, antes da tomada de qualquer decisão com base em dados dos titulares, é necessário que se colha deles o consentimento e acorde os requisitos previstos. Em exemplo concreto, antes do oferecimento de qualquer oferta de produto ou serviço para um cidadão titular de dados tratados por uma empresa, é necessário que haja consentimento prévio, livre, específico e com clara informação acerca da finalidade do uso dos dados por parte dos titulares.

Antes que alguém receba um e-mail, mensagem ou ligação de uma empresa (que o faz tendo acesso aos dados), deve ele ter concordado com aquilo (contato ocasionado pela ciência de dados). Em outras palavras, uma eventual mera exposição das pessoas aos produtos e serviços de determinada empresa, efetivado com base em dados tratados pela instituição (a permitir-lhes melhor alcance de público e mercado), deve ser precedida de autorização lícita para tanto, afinal a oferta (e o direcionamento da oferta) parte do pressuposto de que os dados

são acessíveis ao fornecedor. Tal exigência quanto ao consentimento guarda ainda maior importância quando presente o contexto tecnológico da sociedade de consumo atual, na qual a coleta de dados é possibilitada em massa, mormente se consideradas as instituições financeiras, que não trabalham ocasionalmente com significativa quantidade de clientes que precisam repassar grande quantidade de dados para obter um contrato, apontando Chinellato e Morato (2021. p. 656) que:

> Na sociedade informatizada, digital e globalizada é mais fácil juntar dados isolados que, no conjunto, formam um todo plenamente identificável. Assim, dados esparsos de uma pessoa, uma vez reunidos, podem perfeitamente identificá-la, sem seu consentimento para que tal ocorra.

Não basta, portanto, a simples menção genérica em contrato de "autorização para tratamento", havendo de ser claro e detalhado o deferimento, por parte do usuário/consumidor, da permissão para uso de seus dados em finalidades específicas, incluídas aí o recebimento futuro de novas ofertas de produtos e de serviços. Em estudo correlato de Mendes e Fonseca (2021), anota-se que, segundo os ditames de proteção de dados no país, a usual menção (rotineiramente anotada mediante um "clique" em sítios eletrônicos) à pura leitura e aceitação ("li e aceito") não é suficiente, nem clara e nem específica conforme o adequado. Aliás, não raro é de difícil compreensão a própria extensão de tais termos, assim como não rara também é a condição de aceitação do tratamento para viabilização do acesso ao serviço/produto oferecido.

Dessa maneira, as dificuldades em torno do consentimento (se manipulado ou não, se realmente "livre" e "informado" ou não) levam os estudiosos a refletirem ante os desafios propostos, tais como a ascensão do big data (técnicas de captação, armazenamento e processamento de dados em larga escala para extrair informações[3]), tecnologias de rastreamento e monitoramento de usuários de serviços, desigualdade de poderio entre os contratantes e dependência dos produtos e serviços, entre outros.

Dentre as respostas aos desafios mencionados (MENDES, FONSECA, 2021), menciona-se a inclusão de tecnologias que permitam acesso e controle eficaz por parte dos titulares de dados (em exemplo das mensagens cifradas via criptografia), instituição de

[3] Os autores mencionam em nota de rodapé um conceito resumido de "Big Data" nesse sentido: "O termo Big Data é de difícil definição precisa e taxativa. No entanto, em linhas gerais, segundo os autores, Big Data refere-se às técnicas de captação, armazenamento e processamento de dados em larga escala para extrair novos insights ou criar novas formas de valor, alterando sensivelmente mercados, organizações, as relações entre o Governo e seus cidadãos" (MENDES e FONSECA, 2021, pg. 90).

programas destinados ao gerenciamento da privacidade, incremento de instrumentos que permitam um maior caráter auditável ao manejo de dados, entre outros, para melhor amparar o consentimento e autonomia do cidadão. Enfim, o consentimento sem vícios é "pedra de toque" para exame da licitude do tratamento de dados.

Teixeira e Guerreiro (2022), por sua vez, afirmam que o consentimento garante uma maior transparência e controle ao tratamento, por possibilitar ao agente a segura prova de que a aquiescência foi obtida. Caso o dado seja, posteriormente, tratado por terceiro, será necessário novo consentimento, em acordo ao art. 7º, § 5º, LGPD.

O consentimento, segundo os mesmos autores, também não há de ser conferido segundo opções não precisas ou de difícil compreensão pelo titular. Na mesma toada, a concordância deverá ocorrer em termos compreensíveis, sendo delegada ao proprietário dos dados a mesma facilidade para retirada do consentimento, quando em comparativo à sua obtenção. A título de debate e acorde a experiência comum em uso de internet, por vezes a opção de aceitação de "cookies" em um site é única, sem opção clara de negativa. Ainda, se um "clique" em uma "caixa" possibilita permissão para tratamento, não é por vezes simples a retirada desse consentimento, ou a chance de expressar o arrependimento. Tais temas foram também abordados em decisões por agências de dados europeias (capítulo II deste trabalho).

A necessidade para cumprimento de obrigação legal ou regulatória (inciso II), a seu turno, permite o tratamento dos dados pelo controlador, ainda que sem o consentimento direto do titular. Em exemplificação, pode-se mencionar a necessidade de que um empregador detém de informar órgãos fiscalizadores, tributários, entre outros, acerca de seus funcionários. Ainda assim, por transparência quanto ao uso, há de se informar tais operações ao contratado logo no início de sua relação (TEIXEIRA e GUERREIRO, 2022).

A necessidade para execução de contrato (inciso V) guarda conexão com o próprio fim visado pelo titular. Em exemplo, cite-se a necessidade de se requerer endereço pormenorizado a fim de que um produto seja entregue (TEIXEIRA e GUERREIRO, 2022). A proteção de interesses legítimos do controlador ou de terceiro (inciso IX) pode englobar uma série de fatores correlatos a uma prestação de serviço ou execução contratual.

Teixeira e Guerreiro (2022) apontam que os cuidados de um fornecedor de serviços ou produtos quanto à segurança, no sentido de se evitarem as fraudes, podem ser lícitas e coerentes com a LGPD a depender do contexto. Em exemplificação, a exigência de foto (ou "selfie", mediante fotografia com o celular) pode ser instrumento eficaz para a prevenção de engôdos por intermédio de terceiros, sendo a princípio lícito a exigência dessa espécie de dado pessoal relacionada à imagem.

É claro, ademais, como o próprio inciso IX indica, que há a necessidade de ponderação com os interesses e direitos do titular, a fim de que não se verifiquem abusos. Adiante, a proteção ao crédito (prevista também no inciso X do art. 7º, da LGPD, tem relação com o interesse legítimo do controlador, sendo abordada nestes termos:

> A proteção ao crédito também autoriza o tratamento de dados, garantindo-se o crescimento da economia como um todo e a preservação da sociedade, precedendo o interesse individual do titular, que está inadimplente ou que é um mau pagador. Essa hipótese engloba ainda o tratamento de dados pessoais para compor o score (pontuação, em português) do indivíduo e para a prevenção antifraude a ser adotada pelo agente de tratamento. Assim, não poderá, por exemplo, o titular solicitar a exclusão de seus dados pessoais dos cadastros de restrição ao crédito ou mesmo se negar a fornecer dados pessoais para pleitear financiamento em uma instituição financeira. É de se rememorar que a proteção ao crédito também é vislumbrada na Lei do Cadastro Positivo (Lei n. 12.414/2011), que 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. (TEIXEIRA; GUERREIRO, 2022, p. 22).

1.3.2 Os princípios do tratamento de dados.

O desenvolvimento da tecnologia, especialmente no que se refere aos dados, e as constantes transformações da sociedade, que em seu bojo envolve distintos interesses e setores, são de difícil previsão e acompanhamento pelo legislador. A LGPD prevê uma série de princípios que servem de diretrizes acerca das possibilidades de tratamento de dados, chegando os autores Teixeira e Guerreiro (2022, p. 19) a denominarem a lei geral de proteção de dados de “lei principiológica”.

O art. 6º da LGPD, com esse desiderato, prevê em seus incisos que as atividades de tratamento de dados, além da boa-fé, obedecerão aos seguintes princípios: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas. Para fins do presente trabalho e recorte metodológico, trataremos dos princípios previstos nos incisos I (finalidade), II (adequação) e III (necessidade), chamados de “mínimo essencial” (TEIXEIRA e GUERREIRO, 2022, p. 19), pois garantem, sob seu enfoque, que um mínimo de dados sejam tratados para que se atinjam os lícitos fins pretendidos em qualquer relação.

A finalidade, em primeiro plano, exige que a coleta de dados deve obedecer apenas

à finalidade para a qual foi coletada, ou seja, veda-se o uso de dados para contexto distinto do qual foram eles requisitados (TEIXEIRA; GUERREIRO, 2022).

O princípio é assim descrito no inciso I do art. 6º, LGPD: "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Da leitura do dispositivo se depreende que os objetivos do uso dos dados do titular devem ser delimitados pormenorizadamente pelo controlador desde o início da relação, com a concomitante informação ao titular. Não há, assim sendo, irrestrita liberdade a quem controla os dados, havendo de se guardar no tratamento os estritos propósitos que geraram a sua colheita na origem.

Em caso de alteração dos propósitos, o titular deve ser informado, sendo a ele ainda facultada a revogação do consentimento para tratamento em caso de discordância, conforme art. 9, § 2º, LGPD: "Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações." Ou seja, se a finalidade da coleta era possibilitar o envio de uma mercadoria para um endereço específico, essa finalidade deverá delimitar o uso dos dados, não sendo possível, em exemplo, que esses dados sejam "vendidos" para outra empresa com interesse nas informações, pois essa não era a finalidade informada ao usuário (afora a obtenção de consentimento específico para isso).

Flumignan, S. e Flumignan, W. (LIMA, 2020, p. 129), em didáticas exemplificações, deduzem que a delimitação do interesse lícito e coerente com o propósito inicial é possibilitado mediante a ponderação concreta:

> Em caso hipotético, imagine que um aplicativo de transporte armazene, após o consentimento do usuário, dados com a finalidade precípua de saber onde há maior demanda de usuários por região e quais os destinos que geralmente fazem. Essa empresa não poderá alterar o tratamento de dados pessoais para finalidades diferentes destas sem o prévio e legítimo consentimento dele. Outro exemplo é o de uma startup que solicita o e-mail do cliente para a finalidade específica de login na plataforma. Neste caso, não poderá automaticamente utilizar esse mesmo e-mail para envio de ofertas ou publicidade. De fácil percepção que, a partir da promulgação da LGPD, não é mais possível o tratamento dos dados pessoais com finalidades genéricas ou indeterminadas.

Outro princípio previsto no art. 6º da LGPD, e correlato com o da finalidade, é o princípio da adequação, também previsto no inciso II: "compatibilidade do tratamento com as

finalidades informadas ao titular, conforme o contexto do tratamento". Ou seja, somente são válidos os tratamentos objetivamente compatíveis com a viabilização do fornecimento de um produto ou serviço, sendo vedado o pleito de informação de dados incoerentemente ou sem justificativa, a exemplo do fornecimento de dados sobre a saúde a aplicativos de transporte (LIMA, 2020).

O inciso III do art. 6º, LGPD, por sua vez, conceitua o princípio da necessidade nos seguintes termos: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".

Flumignan, S. e Flumignan, W. (LIMA, 2020) dissertam que o princípio possui duas facetas, pois, a uma, delega ao controlador maior responsabilidade na coleta, porquanto deverá avaliar a estrita necessidade ou não do dado para o negócio, garantindo maior segurança quanto ao vazamento de dados que sequer eram indispensáveis. Noutro vértice, significa uma "minimização do tratamento de dados" (LIMA, 2020, p. 131), pois apenas aqueles dados e informações deveras imprescindíveis à relação jurídica deverão ser tratados.

Em outras palavras, o dado inútil à relação estatuída não deve ser tratado. E não são muitas as orientações nesse sentido destinadas às empresas no Brasil, como se pode verificar junto ao site da Autoridade Nacional de Proteção de Dados (ANPD), quando em comparativo com o European Data Protection Board (EDPB – Comitê Europeu de Proteção de Dados), que apresenta até, em exemplificação do maior detalhismo, diretrizes sobre os limites do necessário para gestão da segurança pública no que toca aos mecanismos de reconhecimento facial[4].

1.3.3 O tratamento de dados pessoais sensíveis, o livre desenvolvimento da personalidade e regulação.

Segundo o artigo 5º, inciso II, LGPD, dado pessoal sensível é aquele que diz respeito à "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". De início, infere-se que os dados pessoais, de forma geral, permitem a identificação da pessoa natural.

[4] "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement". Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

Os dados de natureza sensível, por guardarem relação com opiniões, convicções, origens, entre outros, permitem estruturar perfis, pois tais informações suplantam a simples identificação de um indivíduo. Em artigo sobre o tema, Mulholland (2018) alude que dados sensíveis permitem o "perfilamento", com uso das informações inclusive para tratamento discriminatório (no caso de conotações negativas), considerando o nível de conhecimento que o poder público e mercado podem adquirir sobre os cidadãos, rotulando-os. Ainda, as informações podem incrementar e personalizar a venda de produtos e serviços, com maior desconsideração de sua autonomia.

Assim relata o autor (MULHOLLAND, 2018, p. 166-174):

> [...] a formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação (...) dados pessoais, aparentemente não 'sensíveis', podem se tornar sensíveis se contribuem para a elaboração de um perfil (...) A título de ilustração, dois casos relatam os malefícios do perfilamento (profiling), com uso de dados pessoais que geraram tratamento discriminatório. Os casos ocorreram nos EUA e se referiram à contratação de serviços médicos e de seguridade. No primeiro caso, algumas seguradoras utilizaram dados pessoais relacionados às vítimas de violência doméstica, acessíveis em banco de dados públicos. O resultado do tratamento dos dados levou a uma discriminação negativa, ao sugerir que mulheres vítimas de violência doméstica não poderiam contratar seguros de vida, saúde e invalidez. Em outro caso, relacionado a dados de saúde, 'quando uma pessoa tem um derrame, alguns bancos, ao descobrir tal fato, começam a cobrar o pagamento dos empréstimos realizados.

Esses dados são dotados de valor econômico vez que se constituem em matéria-prima para uso de ferramentas estratégicas, tais quais algoritmos, inteligência artificial ou Big Data (RUARO; SARLET, 2021) e os conhecimentos que esses instrumentos proporcionam sobre as pessoas, a exemplo de uma melhor definição de alvos de mercado, ou mesmo de pessoas mais vulneráveis às ações desenvolvidas.

Nesse sentido, as informações ensejadas pelos dados ditos sensíveis podem ser utilizadas pelas empresas para variadas ofertas de seus produtos e serviços, afinal cada gama de prestação contratual há de guardar relação com características pessoais e de comportamento, para além da identificação de cunho apenas civil. É possível dessarte que a caracterização de alguém como aposentado por invalidez ou idade, através do exame de seus dados sensíveis, eleja-o um alvo de práticas empresariais, mediante tentativa de abordagem de instituições com finalidade de lhe oferecer novos serviços ou empréstimos. Nesse cenário, Simão Filho (2019, p. 193-194) afirma que, a depender do manejo que dele se faça, o banco de dados pode ser tornar um "ativo tóxico" e gerador de problemas à empresa que dele abuse.

Portanto, as informações mais detalhadas do indivíduo demandam uma proteção ainda mais acurada, com atenção à multidimensionalidade da pessoa humana e no respeito ao seu livre desenvolvimento (LIMA, 2020).

Como adiantado, os dados que permitem a identificação de um cidadão como idoso possuem caráter sensível por permitirem uma mínima verificação de perfil, sendo ele por certo mais acessível e vulnerável a determinadas práticas com possibilidades nocivas, a exemplo de superendividamento.

Nesse tópico, é possível que, mediante acesso a dados sensíveis sem o consentimento devido (em desrespeito à LGPD), uma empresa de cunho financeiro envie seguidas propostas de mais empréstimos ou cartões a pessoas aposentadas, ou pensionistas (ou seja, a princípio, solventes se parcelado o débito) e com histórico/perfil de aceitação de novas dívidas, onerando em demasia o cidadão.

Com essa preocupação, o art. 11, LGPD, disciplina as estritas hipóteses em que o tratamento de dados sensíveis poderá ocorrer. Em primeiro ponto, quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades também específicas (artigo 11, I).

Ainda, sem o fornecimento de consentimento do titular, nas hipóteses em que for indispensável para cumprimento de obrigação legal ou regulatória pelo controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); proteção da vida ou da incolumidade física do titular ou de terceiro; tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (artigo 11, inciso II).

Em consonância, em variados trechos da LGPD, o legislador aponta a necessidade de maior cuidado com os dados sensíveis em razão da possibilidade de abuso e dano em prejuízo dos titulares, a exemplo da vedação ao controlador do tratamento de dados de saúde

para prática de seleção de riscos na contratação de plano privado de assistência à saúde (art. 11, § 5º, LGPD). Ruaro e Sarlet (2021), retomando a reflexão de que, para além da simples identificação do indivíduo, os dados sensíveis permitem construir perfis digitais, apontam que tais informações acabam por deter intenso valor não apenas financeiro, mas político, pois se tornam matéria-prima para uma série de ações e possibilidades de controle pelos entes controladores.

O uso de algoritmos, inteligência artificial e big data é fator que torna esse arranjo possível. Ainda, questões como a existência e suficiência do consentimento para junção de dados em nuvens materializadas em servidores ou mesmo o simples vazamento de dados (compartilhamento ilícito e sem consentimento) podem potencializar ainda mais um panorama de manejo abusivo de dados, com prejuízo à dignidade da pessoa humana.

Com essa preocupação, a Organização das Naçoes Unidas (ONU), especialmente após o vazamento de dados ocasionados por Edward Snowden, aprovou resolução acerca da proteção da privacidade na era digital em 2013[5]. Dentre outros, prevê a entidade que ninguém deve sofrer interferência abusiva e ilegal em sua privacidade, abrangidos aí sua família, lar e correspondências; e que as mesmas proteções deferidas em âmbito exterior à internet devem ser delegadas às operações digitais; e, dentre outros, convocou os estados a rever seus procedimentos, práticas e legislações acerca da vigilância das comunicações, interceptação e coleta de dados pessoais, com vistas a fortalecer o direito à privacidade e o implemento dos direitos humanos.

Em abril de 2020[6], a ONU noticiou que, apesar do aumento do número de leis de proteção de dados entre 2015 e 2020, apenas 66% dos países salvaguardam os dados de seus cidadãos, ressaltando a preocupação diante dos aumentos dos crimes cibernéticos, além dos golpes e fraudes praticados online, especialmente após a pandemia[7]. Ao final, acentua a entidade que mais do que a aprovação de leis, devem os estados as aplicarem.

Ruaro e Sarlet (2021) asseveram que a tutela da identidade atua com dois enfoques principais: mediante a tutela da identidade pessoal em si, a envolver seus atributos como honra, imagem, reputação, entre outros, em consideração mais direta ao livre desenvolvimento da personalidade; e, noutro vértice, em atenção aos métodos existentes para

---

[5] Texto disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/resolucao-sobre-o-direito-a-privacidade-na-era-digital

[6] Notícia disponível em: https://news.un.org/pt/story/2020/04/1712072

[7] Segundo artigo publicado na revista Valor Econômico, em 2021 houve 88,5 bilhões de tentativas de ataques cibernéticos em 2021 no Brasil. Disponível em: https://valor.globo.com/patrocinado/dino/noticia/2022/06/27/crimes-digitais-crescem-pos-pandemia-e-provocam-corrida-por-ciberseguros.ghtml.

identificação do sujeito através de seus dados. Assim, enunciam que todo tratamento, no caso de dados sensíveis, deve buscar também ao máximo a quebra do liame entre o dado e a pessoa (cite-se a possibilidade de anonomização, prevista no art. 5º, III, LGPD), diminuindo-se as possibilidades de criação de perfis.

Obviamente, nesse contexto, não é lícito o empreendimento de ferramentas tecnológicas (como algoritmos) para que dados relevantes de uma pessoa sejam coletados sem necessidade, ainda que mediante um ajuste negocial. Do contrário, se os dados sensíveis hão de ser tratados, o consentimento deverá ser o mais claro o possível. Aliás, se a tecnologia for utilizada, tal como os algoritmos e inteligência artificial, deve ela ser utilizada para emancipação da humanidade, com incremento de capacidades cognitivas, sociais e culturais, e não para vigilância ilícita e tratamento do indivíduo como número.

Ainda acerca do raciocínio da proteção dos dados pessoais e do desenvolvimento da personalidade, Doneda (2021b), ao examinar as gerações de leis protetivas de dados, aponta que com o decorrer da história o enfoque da proteção se modificou. Em momentos iniciais, preocupava-se o legislador eminentemente com o não avanço sobre os dados dos cidadãos, impondo-se um dever negativo, e em maior proximidade com a ideia inicial de Warren e Brandeis (1890) no sentido do direito da pessoa ser "deixada só" ou isolada, caso seja de seu desejo. Mais adiante, com o desenvolvimento da tecnologia e da sociedade, "percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua participação na vida social" (DONEDA, 2021b, p. 182).

Estado e entes privados, como empresas, valem-se das informações pessoais e de seu fluxo para funcionamento, valendo a hipotética absoluta negativa de envio de dados por um cidadão basicamente como sua exclusão de algum aspecto da vida social.

Nesse sentido, caso a pessoa não decida ser uma eremita, necessitará enviar dados para efetuar compras de bens e serviços, ingressar em um curso, obter auxílio à saúde, entre outros.

Dessa maneira, Doneda (2021b) aponta que em uma última geração de leis de proteção de dados, preocupa-se o legislador e os executores com a tutela não só da proteção de dados no sentido de se evitar "devassa" em sua vida pessoal, mas também em tutelar e melhor garantir a sua livre e consciente participação nas "fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros" (DONEDA, 2021b, p. 183), afinal tais tratamentos se relacionam com os atos e decisões inerentes à sua vida e ao seu desenvolvimento, em raciocínio correlato com a autodeterminação informativa.

De relevo a menção a trecho elucidativo:

> [...] uma terceira geração de leis, surgida na década de 80, procurou sofisticar a tutela dos dados pessoais, que continuou sendo centrada no cidadão, porém passou a abranger mais do que a liberdade de fornecer ou não seus dados pessoais, preocupando-se também em garantir a efetividade dessa liberdade. A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – buscando o exercício da autodeterminação informativa (DONEDA, 2021b, p. 182/183).

Por último, fixado o avanço da experiência legislativa brasileira com a proteção de dados pessoais mediante o desenlace de legislação específica (LGPD), resta discutir se, ao menos sob determinado recorte, são ou não eficientes os seus comandos. Afinal, além das hipóteses autorizadoras de tratamento e dos princípios, houve a criação de uma Autoridade Nacional de Proteção de Dados (ANPD; arts. 55-A e ss da LGPD), com competência para zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados, fiscalizar e aplicar sanções em caso de desobediência à LGPD, promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados e privacidade, solicitar informes específicos, realizar auditorias, entre outros, conforme previsto no art. 55-J, LGPD.

Além dessas ferramentas delegadas à ANPD, há a previsão de medidas como anonimidade de dados, confecção de relatórios de impacto e indicação de um encarregado pelo tratamento de dados pessoais, a funcionar de elo entre controlador (pessoa que emite decisões sobre os dados), titulares de dados e ANPD, com atribuições de recebimento de reclamações dos titulares, recebimento de comunicações da ANPD e orientação de funcionários (art. 41, LGPD).

Em resumo, há de se verificar se, conquanto existentes medidas novas para proteção, ainda é necessário no Brasil o clássico e usual recurso às ações judiciais para tutela dos dados pessoais, como já sugeriam Warren e Brandeis (1890) séculos atrás, e a despeito de todo o percurso até aqui vivenciado.

Na Europa, em breve análise sobre as orientações e decisões de agências responsáveis por dados[8], é possível verificar (próximos capítulos) que a difusão do conhecimento acerca do que significa proteger dados é significativamente mais ampla,

[8] Apenas em sua página inicial, o "European Data Protection Board" (EDPB) disponibiliza ao leitor um repositório de decisões, opiniões, diretrizes, consultas públicas, entre outros, além das mais diversas publicações, tornando simples o acesso ao conhecimento. Disponível em: https://edpb.europa.eu/edpb_en (consulta em 09/11/2023).

ensejando-se assim maiores possibilidades de que violações a direitos sejam solucionadas antes que as pessoas necessitem do recurso da ação judicial.

É igualmente de rigor o exame de instrumentos que amplifiquem a eficiência da LGPD, seja para melhorar o panorama atual, seja para manter e estabilizar o que de fato funcione acorde os dados coletados, valendo-se para tanto do quanto disposto pelos estudos correlatos à regulação da atividade econômica.

Salomão Filho (2021), em obra basilar sobre o tema, e partindo-se de problemática relativa ao direito concorrencial para a construção de fundamentos para o direito regulatório, aponta que setores carentes de maior regulação não devem apenas ensear, em comportamento substancialmente passivo, por sanções do Estado a comportamentos indevidos e típicos de agentes econômicos. A propósito, dentre tais agentes, no caso, avaliam-se as empresas e empresários que se valem de dados pessoais como ativos. Ao revés, e de forma verdadeiramente ativa, deve o Estado, mediante seus órgãos e autoridades, "impor comportamentos" (SALOMÃO FILHO, 2021, p. 20) acorde a lei e os preceitos econômicos e éticos.

Aliás, ao impor e estabelecer diretrizes comportamentais, amplia-se a difusão do conhecimento econômico (princípio do direito regulatório acorde o autor), tornando-se mais acessível ao cidadão sem formação jurídica a orientação quanto aos seus direitos e forma de exercê-los, e mais transparentes as possibilidades de aplicação de sanção em detrimento de quem com esses parâmetros não se coadune.

Além disso, Salomão Filho (2021) reflete que os objetivos da regulação não se limitam aos princípios concorrenciais, mas também outros objetivos específicos (como higidez de mercado, segurança, entre outros), e com possível caráter redistributivo (preventivo a injustiças e concentrações de poder). Portanto, ao final, discutir-se-á, acorde o recorte dos dados analisados, os potenciais instrumentos regulatórios aptos a auxiliar a maior (ou mais estável) eficiência da LGPD e, claro, a maior (ou mais estável) tutela ao indivíduo e suas projeções de personalidade.

2 EFICIÊNCIA DA LGPD: comparação com a experiência europeia

Em estudo sobre as tendências e desafios relacionados à proteção de dados pessoais, Zanatta e Souza (2019, p. 384-385) escrevem sobre o "fracasso do modelo contratualista na teoria da privacidade e a análise contextual." Consoante os avanços da tecnologia da informação, e a formação de bancos de dados que permitem encontrar "tudo em qualquer lugar", defendem uma revisão crítica do que significa proteger a privacidade. Citam, no artigo, a coleta por empresa de consultoria política de dados constantes na rede social *Facebook* que permitiu o recolhimento de informações de dezenas de milhões de pessoas, acrescidas de detalhes como gostos, locais visitados, amigos e preferências políticas acorde as "curtidas".

Por óbvio, tais finalidades (uso político) não compunham o objetivo inicial dos usuários da rede social. Afora o debate de eventual permissividade ou não da empresa responsável pela rede quanto ao acesso dos dados por terceiros, fato é que o ajuste de vontades consistente no aviso sobre o uso de dados seguido de consentimento sobre essa prática pouco diz sobre a efetiva proteção da privacidade do indivíduo, de sua privacidade e de seus dados pessoais. A aquiescência ("eu aceito") quanto aos avisos, concluem, não garante respeito e transparência.

Assim, caso se admita como livre a aceitação genérica de tratamento de dados pelas empresas, em uma perspectiva meramente formal e de cunho "civilista" (no sentido de avaliação da liberdade apenas no que toca à aceitação), possivelmente a tutela das projeções da individualidade do cidadão, aí incluídas a proteção de seus dados, não será efetiva. E os problemas daí resultantes, por sua vez, são passíveis de serem apresentados aos Tribunais.

Em artigo publicado recentemente sobre os primeiros cinco anos de vigência da LGPD (JOTA, 2023), apontou-se que esse início foi caracterizado por insegurança do mercado e desconhecimento por parte da sociedade civil. Essas circunstâncias, somadas à maior conscientização sobre o tema, gerou aumento de 500% no número de ações judiciais que discutem o tema proteção de dados, apontando-se também que a maior parte das empresas (oito em cada dez) ainda não se adequaram à Lei Geral de Proteção de Dados, havendo ainda óbices que impedem uma absorção mais célere aos comandos protetivos.

Os maiores desafios, concluem, residem na difusão das informações, na maior conscientização dos cidadãos e na maior assimilação das empresas, mediante uma regulação que se oriente, primordialmente, por um caráter orientador e preventivo. Nessa toada, hipoteticamente, uma redução dos problemas gerados pelo desrespeito aos dados pessoais dos indivíduos passa pelo melhor conhecimento e orientação por parte das empresas e pessoas que convivem no mesmo ambiente regulado.

Diante desse panorama, há de se avaliar se a vigência da LGPD, considerando como recorte principal a atuação de empresas voltadas à telefonia e à área financeira, contribuiu ou não para a redução da litigiosidade nas cortes de justiça. Também, se os métodos atualmente empreendidos para resolução dos problemas dessas empresas com as pessoas, especialmente no que toca ao envio de publicidade e contratações a envolver transferência de dinheiro, são eficazes e coerentes com os ditames da LGPD, acorde a compreensão atual do que significa tutelar o cidadão mediante proteção de seus dados pessoais. Em desfecho, é necessária a comparação com a experiência europeia (que inspirou a realidade brasileira), na tarefa de encontro de uma hipótese para os entraves detectados.

2.1 Tratamento indevido de dados pessoais e processos judiciais no Brasil.

Para recorte do campo de exame da possível eficiência ou não da LGPD, serão examinados de início materiais relacionados ao tratamento de dados em operações de telemarketing, mais especificamente no que toca à abordagem efetuada por empresas de comunicação a potenciais adquirentes de serviços e pelas instituições financeiras aos possíveis contratantes de empréstimos e seguros (principalmente aposentados e pensionistas). Tal separação se faz necessária, pois inviável o exame da eficiência da LGPD sobre todas as possíveis áreas submetidas à sua influência e regulação, bem como porque nas duas situações mencionadas a coleta, uso e tratamento de dados de cidadãos pelas empresas é de grande valor (dado como um ativo), restando ao final mais facilitada a tarefa de verificação de adequação das práticas empreendidas à lei de dados ou não, especialmente no que tange à exigência de consentimento prévio e obediência aos princípios abordados no presente estudo, sobretudo os da finalidade, adequação e necessidade.

Igualmente, há de se avaliar se a resposta dada a esses problemas, na prática, acompanha ou não o percurso evolutivo do legislador no que concerne ao atual paradigma de tratamento de dados fixado em lei, em outras palavras, se o percurso em âmbito teórico é ou não acompanhado nesses casos da eficiência em âmbito concreto.

Depreende-se que o uso excessivo de ligações de telemarketing por empresas do setor de telecomunicações e instituições financeiras (operações de empréstimo consignado e cartão de crédito consignado bancário) motivou a criação, pela Agência Nacional de Telecomunicações (Anatel), de uma lista nacional denominada “Não Me Perturbe”[9],

[9] Disponível em: https://www.gov.br/anatel/pt-br/consumidor/telemarketing/nao-me-

disponível no endereço www.naomeperturbe.com.br.

Segundo a Anatel, a referida lista é apropriada para quem não deseja mais receber ligações de telemarketing de empresas cadastradas, e até agosto de 2022 contava com o cadastro de 5,7 milhões de usuários e 5,6 milhões de números telefônicos incluídos, e prevê bloqueio de ligações em trinta dias após a solicitação. Segundo informações constantes do específico site da lista (mencionado retro), ela foi criada em 16 de julho de 2019 por iniciativa da Anatel, e engloba uma longa série de empresas das áreas de telefonia e financeira[10]. Além disso, um grupo de 8 empresas de telefonia[11] ainda subscreveu em 25 de março de 2019 um código de conduta para ofertas de serviços de telecomunicações por meio de telemarketing, com previsão de variadas limitações ao seu uso, a envolver principalmente: o respeito à vontade do consumidor em caso de contrariedade ao recebimento das ligações; a não realização de ligações sob pretexto de pesquisa ou sorteio quando o objetivo for a comercialização de ofertas; não realização de ligações que não permitam a identificação dos códigos de acesso utilizados pela empresa; não finalizar ligações abruptamente sem identificação da empresa; não empreender ligação em horários de repouso e em domingos e feriados; não efetuar ligações de forma insistente, limitadas a quinze ligações no mês e não realizar chamadas a cobrar aos consumidores.

Acorde esse primeiro recorte regulatório efetuado pela Anatel acerca de ligações relacionadas a telemarketing, alguns pontos devem ser destacados à luz da LGPD. Em primeiro plano, há de se destacar que, muito embora a LGPD tenha sido promulgada em 14 de agosto de 2018 e esteja em plena vigência desde agosto de 2020 (*vacatio legis* prevista em seu art. 65), há informe de que até agosto de 2022 existiam 5,7 milhões de pessoas incomodadas com ligações de telemarketing. Ou seja, existiam 5,7 milhões de pessoas que não forneceram consentimento para uso de seus dados para fins de recebimento de ofertas, em práticas contrárias ao previsto nos artigos 6, inciso I (finalidade), 7, inciso I (consentimento), e 9, inciso I (finalidade), da LGPD. Portanto, ineficiente a LGPD nesse ponto, pois sua vigência e suas

---

perturbe#:~:text=A%20plataforma%20%E2%80%9CN%C3%A3o%20Me%20Perturbe,Lista%20Nacional%20de%20N%C3%A3o%20Perturbe%E2%80%9D.

[10] Segundo o constante do site "www.naomeperturbe.com.br", as empresas participantes da lista são: Algar, Net – Claro, Oi, Sercomtel, Sky, Tim e Telefônica – Vivo, Agibank, BMG, BRB, BV, Banco Alfa, Banco C6 Consignado, Banco Master, Banco do Brasil, Bancoob, Banpará, Banrisul, Bari, Bradesco, Bradesco Financiamentos, CCB Brasil, CCB Brasil Financeira, Cetelem-BNP, Caixa, Daycoval, Digio, Facta Financeira, Financeira Alfa, Inter, Itaú Consignado, Itaú-Unibanco, Mercantil do Brasil, Mercantil do Brasil Financeira, PAN, Paraná Banco, Safra, Santander/Olé e Zema Financeira.

[11] Segundo o disponível em "https://conexis.org.br/wp-content/uploads/2021/02/CT_CodigoCondutaTlmkt_cartacodigo_assinados.pdf", grupos Algar, Claro, Oi, TIM, VIVO, SKY, SERCOMTEL e NEXTEL.

ferramentas, disponíveis em sua plenitude desde agosto de 2020 (sem contar o prazo de vinte e quatro meses para adaptação), não foram suficientes para impedir o indevido uso de dados mediante envio de oferta para quem, a princípio, com isso não concordou e disso não foi devidamente informado. Houvesse respeito à LGPD, questionável seria a própria existência de uma lista denominada "não me perturbe", afinal, por óbvio, quem não consentiu com a coleta de seus dados por uma empresa para fins de recebimento de ofertas, ou não consentiu com o específico uso de dados já fornecidos para fins de recebimento de ofertas, não deveria as receber e menos ainda ter a necessidade de se inscrever em canal "repressivo" das condutas de terceiros. Em consulta ao endereço eletrônico da ANPD[12], em aba relacionada às publicações, verifica-se que inexiste regulação nessa seara (o que seria recomendável a princípio, considerando a magnitude do número de pessoas descontentes com o uso de seus dados para fins de telemarketing).

Resta ainda analisar se a existência de medidas administrativas da Anatel e a vigência da LGPD ao menos refrearam demandas judiciais relacionadas ao telemarketing, segundo utilização de critério de pesquisa baseado nas ligações de cunho indevido.

Em pesquisa realizada perante o sítio eletrônico do Tribunal de Justiça do Estado de São Paulo (TJSP) mediante o uso dos parâmetros "telemarketing" e "ligações"[13], foram listados 1.045 (mil e quarenta e cinco) processos (com uso do filtro de "acórdão", excluindo-se da pesquisa as homologações de acordo, as decisões monocráticas e os Colégios Recursais), sendo o mais recente publicado em 18/08/2023 (TJSP; Apelação Cível 1000930-27.2022.8.26.0326), um dia antes da data da pesquisa de fato (19/08/2023). Para efeito de comparação, nessa mesma pesquisa, quando adicionados filtros temporais, encontrou-se o número de 54 (cinquenta e quatro) processos contendo estes mesmos termos durante o ano de 2017 (ano anterior à promulgação da LGPD); 77 (setenta e sete) processos durante o ano de 2018 (ano da vigência da LGPD); 75 (setenta e cinco) processos durante o ano de 2019; 81 (oitenta e um) processos durante o ano de 2020; 130 (cento e trinta) processos durante o ano de 2021; 156 (cento e cinquenta e seis) processos durante o ano de 2022; e 103 processos durante o ano de 2023 (pesquisa realizada em agosto de 2023, portanto sem contemplar o ano todo). Por transparência, há de se mencionar que a mencionada pesquisa contém, de fato, margem de erro, afinal há casos em que as expressões "telemarketing" e "ligações" são usadas

[12] Consulta realizada em 19/08/2023 no endereço "https://www.gov.br/anpd/pt-br/documentos-e-publicacoes".

[13] Consulta realizada em 19/08/2023 no endereço "https://esaj.tjsp.jus.br/cjsg/consultaCompleta.do?f=1", com uso dos parâmetros "telemarketing" e "ligações", valendo-se do filtro "E", para pesquisa de julgados que contivessem os dois termos.

em contexto distinto da realização de telefonemas indesejados, bem como que não se distinguem os processos com declaração de procedência aos consumidores/titulares de dados, além de não serem abrangidos ademais os processos em que houve desistência, acordo e extinção sem julgamento do mérito.

Ainda assim, é indicativo mínimo do volume em que estes temas surgem no TJSP, e se depreende dela (pesquisa) que a procura pelos Tribunais nos casos de uso indevido de dados para envio de ofertas por ligações não está diminuindo, conquanto desde 2018 exista a LGPD.

Se a mesma pesquisa for empreendida com alteração da origem, excluindo-se o segundo grau, e incluindo-se os Colégios Recursais (sistema dos Juizados Especiais, conforme lei 9.099/95), os resultados são também relevantes.

O total de processos encontrados na mesma data remonta a 580 (quinhentos e oitenta), sendo 33 (trinta e três) durante o ano de 2017; 22 (vinte e dois) no ano de 2018; 36 (trinta e seis) durante o ano de 2019; 33 (trinta e três) no ano de 2020; 32 (trinta e dois) durante o ano de 2021; 49 (quarenta e nove) no ano de 2022; e 71 (setenta e um) durante o ano de 2023 (pesquisa realizada em agosto de 2023, antes do término do ano). Ou seja, com as mesmas ressalvas já feitas quanto à margem de erro, vê-se que, no mínimo, o apelo aos Tribunais não diminuiu com o avanço legislativo. Enfim, nessa temática de uso indevido dos dados para telemarketing, a vigência da LGPD pouco apresentou de eficiência. Dessa forma, é importante notar que, apesar de o tratamento dos dados pelo legislador brasileiro ter avançado, com a promulgação de uma lei específica com novas e diversas ferramentas, ainda é relevante (senão necessário) o tradicional recurso de propositura de demandas perante o Poder Judiciário, solução indicada por Warren e Brandeis (1890), sem o auxílio relevante dos recursos atuais da LGPD, uma vez que o tema ainda é discutido na Justiça. Tomem-se, por exemplo, alguns recursos inominados recentemente interpostos perante os Colégios Recursais do estado do São Paulo (que recebem causas de menor complexidade), cujas ementas narram situações de nítida violação ao consentimento dos usuários quanto ao uso de seus dados:

> Ação de obrigação de fazer cumulada com indenização por danos morais. Telemarketing. Ligações excessivas e reiteradas que causaram incômodo e perturbação. Número de ligações que ultrapassa o limite do aceitável/tolerável. Responsabilidade civil. Danos morais configurados e arbitrados em R$ 3.000,00. Tutela de urgência concedida para fim de fazer cessar as ligações publicitárias. Sentença reformada. Recurso parcialmente provido. (TJSP; Recurso Inominado Cível 1000787-83.2022.8.26.0602; relator (a): André Luis Adoni; Órgão Julgador: 1ª Turma; Foro de Sorocaba - 1ª Vara do Juizado Especial Cível; Data do Julgamento: 23/11/2022; Data de Registro: 23/11/2022).

> RECURSO INOMINADO — Ação de obrigação de não fazer c/c danos morais — Ligações telefônicas excessivas — Utilização de chamadas telefônicas para oferecimento de produtos/serviços bancários, incluindo-se ligações reiteradas e em curto espaço de tempo, que consubstancia prática comum no segmento — Verossimilhança das alegações autorais – Inversão do ônus probatório — Recorrente que não fez prova de suas alegações – Cobrança abusiva e vexatória — Danos morais devidos – Fixação em patamar razoável, considerando-se as circunstâncias do caso concreto – Sentença mantida por seus próprios fundamentos – RECURSO DESPROVIDO. (TJSP; Recurso Inominado Cível 1005697-88.2022.8.26.0268; Relator (a): Daniele Machado Toledo; Órgão Julgador: 4ª Turma Cível, Criminal - Itapecerica da Serra; Foro de Itapecerica da Serra - Juizado Especial Cível e Criminal; Data do Julgamento: 03/08/2023; Data de Registro: 03/08/2023).

> Recurso inominado. Telefonia. Ligações de telemarketing excessivas. Ausência de indicação dos números chamadores que estariam causando o incômodo e que pertenceriam à requerida. Sentença de improcedência que deve ser mantida por seus próprios fundamentos, nos termos do art. 46 da Lei 9.099/95. Recurso da requerente a que se nega provimento. (TJSP; Recurso Inominado Cível 1000604-67.2023.8.26.0541; Relator (a): Adílson Vagner Ballotti; Órgão Julgador: 3ª Turma Cível e Criminal; Foro de Santa Fé do Sul - Vara do Juizado Especial Cível e Criminal; Data do Julgamento: 31/07/2023; Data de Registro: 31/07/2023).

Como se extrai dos precedentes judiciais, há relato de uso abusivo dos dados em patamar que ultrapassa o tolerável e reconhecimento desse tipo de abordagem como comum nesse segmento. Inclusive, no Recurso Inominado Cível 1000604-67.2023.8.26.0541, mencionado acima, há menção pelo julgador da inexistência de indicação do número de chamadores, e praticada por empresa que assinou o código de conduta para instituições de telefonia, conforme abordado no início do tópico.

Assim sendo, houvesse prévia coleta de dados mediante consentimento do usuário para fins de recebimento de ofertas, não haveria sentido, ao menos a princípio, para a existência desse gama de demandas, afinal se o usuário consentiu previamente com o tratamento efetuado pela empresa, dela não teria do que reclamar (menos ainda ao Judiciário).

Por outro lado, se não mais desejasse o consumidor o recebimento das propostas, e claro, se a LGPD estivesse sendo corretamente aplicada, bastaria revogar o consentimento antes de ingressar em juízo, o que igualmente haveria de diminuir o litígio. Obviamente, não se está dizendo que todos os processos relacionados a telemarketing e ligações indesejadas se encerrassem por completo caso respeitada a LGPD, mas sim que a não diminuição da busca pelo Judiciário nesse tema é indicativo de diminuta eficiência.

Acrescente-se ao tópico, e a título de outro exemplo, que nos julgados "TJSP; Recurso Inominado Cível 1002399-98.2022.8.26.0297; Relator (a): Heitor Katsumi Miura; Órgão Julgador: 2ª Turma Cível e Criminal; Foro de Jales - Vara do Juizado Especial Cível e

Criminal; Data do Julgamento: 18/08/2023; Data de Registro: 18/08/2023" e "TJSP; Recurso Inominado Cível 1002821-39.2023.8.26.0297; Relator (a): Mauricio Ferreira Fontes; Órgão Julgador: 2ª Turma Cível e Criminal; Foro de Jales - Vara do Juizado Especial Cível e Criminal; Data do Julgamento: 18/08/2023; Data de Registro: 18/08/2023)" foram reconhecidas as práticas de ligações reiteradas e indevidas para fins de telemarketing, havendo de se pontuar que a empresa responsável por tais práticas também figura como signatária do Código de Conduta para Ofertas de Serviços de Telecomunicações por meio de Telemarketing (mencionado no início deste tópico), a tornar ainda mais sobressalente o vácuo de eficiência da LGPD nessa seara, afinal se mostra recorrente o ilícito uso de dados dos destinatários dos telefonemas.

Ainda no tema de telemarketing, é imperiosa a análise de um dos reflexos de uma abordagem indevida a cidadãos e em descompasso com a LGPD, a qual é o ajuste de contratos senão indesejados, ao menos mal compreendidos.

Mencione-se trecho da ementa (julgado constante da pesquisa retro):

> Ação declaratória de inexistência de débito com pedido de indenização por danos material e moral. Sentença de parcial procedência para declarar a inexistência de relação jurídica, condenar o réu a indenizar pelo dano moral em R$5.000,00 e à repetição em dobro do indébito. Recurso de ambas as partes. Apelo do réu pela improcedência da demanda. Alternativamente, pretende que a repetição do indébito se dê de forma simples e que seja reduzido o valor da indenização. Recurso adesivo da autora para ver majorado o valor da indenização. Empréstimo consignado. Não demonstrada a clareza da contratação, necessária à efetivação do negócio jurídico. Áudio trazido aos autos que demonstra que a autora foi induzida dolosamente a erro pela preposta do réu e não tinha interesse na contratação de empréstimo. Vício de consentimento demonstrado. Réu que não se desincumbiu de seu ônus probatório. Débito inexigível. Retorno das partes ao 'status quo ante'. Necessidade de devolução da importância descontada indevidamente do benefício da autora, assim como do valor creditado em seu favor, sob pena de enriquecimento ilícito. Restituição da quantia descontada do benefício da autora que se dará na forma dobrada. Entendimento fixado em sede de recurso repetitivo pelo STJ (EAResp 676608/RS). Modulação temporal dos efeitos do novo entendimento. Autorizada a compensação. Dano moral. Elaboração fraudulenta de contrato em nome da autora que foi ludibriada pela preposta do réu. Desconto indevido em seu benefício previdenciário. Verba de caráter alimentar. Falha na prestação de serviço. Responsabilidade objetiva do banco. Inteligência do art. 14 do CDC. Súmula 479 do STJ. Autora que buscou a devolução do valor de imediato. Dano moral reconhecido. 'Quantum' fixado na importância de R$ 5.000,00 que é o suficiente para cumprir suas funções – indenizatória, preventiva e punitiva. Princípios da razoabilidade e proporcionalidade atendidos. Sentença mantida. Recursos desprovidos. (TJSP; Apelação Cível 1000930-27.2022.8.26.0326; Relator (a): Virgilio de Oliveira Junior; Órgão Julgador: 23ª Câmara de Direito Privado; Foro de Lucélia - 1ª Vara; Data do Julgamento: 18/08/2023; Data de Registro:

18/08/2023).

Em exame ao julgado acima, verifica-se que a consumidora, em momento seguinte ao recebimento de uma oferta não previamente requerida por ela, termina por realizar um contrato indesejado. No caso[14], não só não desejava a consumidora o recebimento de específicas ofertas de novos empréstimos, como, por óbvio, não desejava a princípio o novo empréstimo em si, e terminou ludibriada.

Nesse ponto, tem-se que dois problemas significativos foram causados: i) o primeiro, foi o envio de oferta sem aparente aquiescência, porquanto a autora, ao menos segundo se depreende dos autos, não apresentou comportamento e resposta coerentes com quem, de forma livre e consciente, consentiu com o uso de seus dados para fins de recebimentos de novas ofertas (princípio da finalidade); ii) o segundo, foi o final ajuste de um contrato em verdade indesejado. Consequentemente, partindo-se da pesquisa sobre ofertas enviadas via telemarketing em descompasso com a LGPD, encontra-se exemplo de caso em que a violação de direitos relacionados aos dados gerou problema que não se exauriu na pura violação à lei de dados, pois o contrato que "nasceu" dessa proposta forçada também foi problemático e, em última análise, pouco ou não realmente desejado.

Por óbvio, quem não consente, e consequentemente, não se interessa em saber de novas possibilidades de contrato com uma instituição, a princípio e obviamente não quer o ato final: o próprio contrato.

Assim sendo, diante de uma abordagem em colisão com a LGPD e seus princípios, incrementa-se, ao menos em teoria, as chances de criação de um problema que não raro exigirá recurso à Justiça: a rescisão de um contrato. Vulnera-se aqui em essência o direito de participação livre e consciente do cidadão na sucessão de tratamento de seus dados, como afiançado por Doneda (2021b), em análise das gerações de leis de proteção de dados.

Então, não bastassem as possibilidades (em tese desnecessárias, caso houvesse conformidade com a lei) de demanda com vistas a encerrar diretamente o tratamento de dados de forma não consentida (a exemplo das ligações excessivas), incrementa-se o risco da existência de mais uma demanda para "conserto" final de todo o problema gerado (rescisão), em recorrente apelo do uso clássico de ações judiciais, como sugeriram Warren e Brandeis

[14] "Conforme se observa do áudio de fl. 174, funcionário de telemarketing da ré, em ligação telefônica, informa a autora de que 'estaria devolvendo um valor a título de juros abusivos'. Nada é dito sobre a contratação de um novo empréstimo, sendo reiterado, por diversas vezes, que ocorreria apenas devolução de valores referentes a cobrança de juros abusivos em empréstimos anteriores." (texto do voto da Apelação Cível 1000930-27.2022.8.26.0326, disponível para consulta no site "www.tjsp.jus.br", na consulta de jurisprudência).

(1890) na origem dos estudos do direito à privacidade, passando-se ao largo de instrumentos regulatórios ínsitos à LGPD.

Outro exemplo de conduta abusiva no trato de dados é o caso descrito na Apelação Cível 1001704-97.2019.8.26.0185 (TJSP), também colhido na pesquisa descrita no início do tópico, que apresenta no mínimo duas violações aos direitos do cidadão, afora a final tutela judicial obtida no final do julgamento, com declaração de rescisão. Vejamos a ementa:

> CIVIL. SEGURO. CONTRATAÇÃO POR MEIO DE LIGAÇÃO TELEFÔNICA. AUSÊNCIA DE ASSENTIMENTO VÁLIDO. PRÁTICA ABUSIVA À LUZ DO ART. 39, IV, CDC. RESTITUIÇÃO SIMPLES DOS PRÊMIOS. DANO MORAL CARACTERIZADO. INDENIZAÇÃO MANTIDA DIANTE DA HIPÓTESE CONCRETA. 1. A partir do link disponibilizado, é possível constatar que a oferta verbal não delimita de forma objetiva sua natureza comercial, sendo certo que a atendente utiliza as informações privilegiadas obtidas de terceiro para inculcar a ideia de que a autora estava recebendo um benefício por sua boa relação com instituição financeira onde recebe sua pensão mensal. 2. Não há contrato de seguro validamente formado, sendo devida a restituição, embora simples, dos prêmios descontados, corrigidos e acrescidos de juros de cada desconto, posto não se cogitar de responsabilidade civil contratual diante da declaração de inexistência de relação jurídica. 3. Há dano moral a ser ressarcido uma vez que a forma como se deu a abordagem da autora denota elevado grau de reprovabilidade da conduta, posto haver informações relacionadas à idade e renda mensal da autora, que haveria de comprometer parcela significativa de seus proventos para custeio dos prêmios mensais do seguro. 4. Recurso parcialmente provido. (TJSP; Apelação Cível 1001704-97.2019.8.26.0185; Relator (a): Artur Marques; Órgão Julgador: 35ª Câmara de Direito Privado; Foro de Estrela D'Oeste - 1ª Vara; Data do Julgamento: 20/07/2020; Data de Registro: 20/07/2020).

Na hipótese mencionada, a autora recebia pensão por intermédio de uma determinada instituição bancária, quando percebeu o início de descontos efetuados nos seus valores por ocasião do pagamento de um seguro, desconhecido por ela. Em minucioso exame, o desembargador relator menciona link específico dos autos (disponível no bojo do texto do acórdão) por meio do qual se denotam duas condutas da empresa seguradora que cobrava os prêmios relativos ao contrato de seguro desconhecido: primeiro, do cenário se depreende que a abordagem à pensionista foi realizada por telefone; segundo, o julgador aponta que:

> [...] a atendente utiliza as informações privilegiadas obtidas por terceiro para inculcar a ideia de que a autora estava recebendo um benefício por sua boa relação com instituição financeira onde recebe sua pensão mensal.[15]

[15] Texto disponível no corpo do acórdão do julgado "TJSP; Apelação Cível 1001704-97.2019.8.26.0185; Relator (a): Artur Marques; Órgão Julgador: 35ª Câmara de Direito Privado; Foro de Estrela D'Oeste - 1ª Vara; Data do Julgamento: 20/07/2020; Data de Registro: 20/07/2020", disponível no site "www.tjsp.jus.br".

Em resumo, e conforme se ouve do áudio, a funcionária aponta que a empresa seguradora é "parceira"[16] do banco com a qual a autora tem relação, e de início já afirma que a razão é o ótimo relacionamento da pensionista com a instituição financeira. Sem maiores questionamentos, a telefonista já passa à descrição do contrato de seguro a ser ajustado, com menção a capital, parcelas, coberturas, entre outros. Em seguida, descreve os dados da autora, como endereço, CPF e data de nascimento.

Ao final, sequer pergunta se ela aceita o contrato, mencionando apenas uma breve pergunta como "sim?", sendo claro que a cliente nada entendeu da ligação. Enfim, a par do reconhecimento da ilegalidade do contrato, ao passo que o Tribunal reconheceu que as informações foram pouco claras, ao menos duas violações à LGPD aconteceram.

A uma, a própria abordagem para recebimento de oferta de contrato de seguro. Da leitura se percebe que a pensionista era cliente do banco, e não da seguradora. Assim sendo, não é crível que a seguradora tenha obtido os dados diretamente da pensionista, afinal ela não detinha seguro e não era cliente dela, mas do banco. Consequentemente, é relevante a possibilidade de que ela tenha obtido os dados dela por meio do banco sem autorização. Vale dizer, é nítida a possibilidade que o banco tenha repassado os dados à seguradora, pois do contrário seria difícil à empresa de seguros obter tantos dados da pensionista e ainda saber do bom relacionamento dela com o banco. E, para uma empresa transferir os dados de um cliente para outra, é necessário consentimento, e ofertado de forma livre, clara e consciente. Adiante, mesmo que de posse lícita dos dados, o tratamento deles haveria de ser limitado segundo determinadas finalidades previamente informadas. Se a pensionista mal entendeu o caráter da ligação/proposta, é porque muito provavelmente não consentiu validamente para o uso de seus dados para fins de envio de novas ofertas e oportunidades por determinada empresa. Ademais, não houvesse a dupla violação à LGPD, com transferência indevida de dados e oferta de serviço sem que essa faculdade tivesse sido acordada validamente, desnecessário seria o processo, ora mais uma vez utilizado, embora existentes mecanismos regulatórios outros. Conforme será estudado em tópico posterior, houve casos na Europa em que o mero envio de mensagens contendo publicidade gerou a aplicação de sanção a empresas. Conquanto não se esteja a definir que uma sanção a uma empresa com base em violação à LGPD tudo resolva, é deveras razoável que esse tipo de comportamento seja repreendido cada vez mais.

Em exame à abrangência do problema mencionado no acórdão examinado, em pesquisa

[16] Conforme áudio, o banco mencionado é o Bradesco, e a empresa seguradora, que é parte no processo, é de nome "Seguradora Sabemi S/A".

empreendida no site do Tribunal de Justiça do Estado de São Paulo (TJSP), a envolver termos relacionados às duas instituições chamadas pela telefonista de "parceiras", extrai-se a existência de 569 (quinhentos e sessenta e nove processos), isso compreendendo o relativamente curto período de 2018 a 2023[17]. Embora a pesquisa detenha margem de erro, sendo possível que aí se incluam menções a esses termos sem que eles sejam o cerne do tema, o número não é desprezível. Não apenas não é, como indica que a problemática não é circunstancial, nem isolada e menos ainda fortuita, em indicador sério de malversação de dados de clientes pelas "parceiras". As reclamações de "descontos indevidos" usualmente se referem a benefícios previdenciários, sendo os beneficiários uma espécie de "alvo" para aquisição de novos contratos por empresas (no mesmo sentido do abordado "perfilamento"). O resultado, de forma indiciária, é a litigiosidade decorrente da prática, sem que sequer se proceda à pesquisa em outros Tribunais da federação, no intuito de não abranger por demais a pesquisa da dissertação. Aliás, se a pesquisa detiver termos modificados, para abranger outras empresas, com menção apenas a "descontos indevidos", "pensão" e "seguro", o número sobe para 2.522 (dois mil, quinhentos e vinte e dois processos)[18].

O TJSP em outras decisões, e em contexto semelhante, reconheceu o pertencimento de determinada instituição bancária e outra de prestação de serviços odontológicos[19] em processos que impugnavam a contratação desses serviços, bem como os descontos empreendidos em contas bancárias gerenciadas pelo banco. Em quatro dessas decisões[20] o Tribunal reconheceu como indevidos os descontos efetuados em conta bancária de correntistas de determinado banco a título de um plano específico de saúde odontológico, tido por nunca contratados pelos autores dos processos. Ou seja, se o cliente do banco não reconhece a contratação de serviço de saúde com uma empresa que, ao menos até a ocorrência dos

[17] Pesquisa realizada em 26/08/2023, na aba de "consulta de jurisprudência" do TJSP, utilizando-se dos seguintes termos: "Bradesco", "Sabemi" e "descontos indevidos", todos interligados pelo filtro "E", com intenção de encontro de julgados que acumulem os três termos.

[18] Pesquisa realizada em 26/08/2023, na aba de "consulta de jurisprudência" do TJSP, utilizando-se dos seguintes termos: "descontos indevidos", "pensão" e "seguro", todos interligados pelo filtro "E", com intenção de encontro de julgados que acumulem os três termos

[19] Pesquisa com os termos "Bradesco", "Odontoprev" e "grupo econômico" (este último termo na aba da "ementa"), na data de 28/08/2023.

[20] TJSP; Apelação Cível 1000127-68.2022.8.26.0027; Relator (a): José Carlos Ferreira Alves; Órgão Julgador: 2ª Câmara de Direito Privado; Foro de Iacanga - Vara Única; Data do Julgamento: 21/04/2023; Data de Registro: 21/04/2023; Apelação Cível 1068694-90.2021.8.26.0576; Relator (a): Schmitt Corrêa; Órgão Julgador: 3ª Câmara de Direito Privado; Foro de São José do Rio Preto - 7ª Vara Cível; Data do Julgamento: 31/03/2023; Data de Registro: 31/03/2023; TJSP; Apelação Cível 1003541-90.2016.8.26.0704; Relator (a): Elcio Trujillo; Órgão Julgador: 10ª Câmara de Direito Privado; Foro Regional XV - Butantã - 2ª Vara Cível; Data do Julgamento: 12/12/2017; Data de Registro: 14/12/2017; e Apelação Cível 1020611-92.2016.8.26.0196; Relator (a): Silveira Paulilo; Órgão Julgador: 21ª Câmara de Direito Privado; Foro de Franca - 2ª Vara Cível; Data do Julgamento: 19/10/2017; Data de Registro: 19/10/2017.

descontos em seu dinheiro, ele não conhecia, é patente que a instituição financeira repassou os dados do seu correntista à empresa de saúde. Mais patente se torna essa hipótese se a Corte de julgamento afirma que pertencem ao mesmo grupo, depois da análise de informações na internet e dos elementos dos autos. Nesse sentido:

> APELAÇÃO. DECLARATÓRIA DE INEXISTÊNCIA DE RELAÇÃO CONTRATUAL C.C. DANOS MATERIAIS E MORAIS. Sentença que acolheu os pedidos, para declarar inexistência de contratação de plano odontológico e condenar as rés a restituir mensalidade debitada da conta bancária do autor, além de pagar indenização por danos morais fixados em R$ 3.000,00. Aplicação do CDC. Ilegitimidade passiva afastada. Documento emitido por Bradesco Seguros no qual afirma que Odontoprev, em conjunto com Bradesco Dental, integram o mesmo grupo econômico. Contestação que não impugna o documento. Conversa de Whatsapp na qual o banco Bradesco indica o número telefônico de Odontoprev/Dental Bradesco, para cancelar contrato e requerer o reembolso da quantia debitada. Atuação conjunta das rés. Mérito. Rés que não comprovaram a contratação. Ilicitude do débito que autoriza a restituição da quantia e o ressarcimento de danos morais, os quais se dão em "ré ipsa". Arbitramento razoável e proporcional. Sentença confirmada por seus próprios e jurídicos fundamentos. Recurso não provido. (TJSP; Apelação Cível 1068694-90.2021.8.26.0576; Relator (a): Schmitt Corrêa; Órgão Julgador: 3ª Câmara de Direito Privado; Foro de São José do Rio Preto - 7ª Vara Cível; Data do Julgamento: 31/03/2023; Data de Registro: 31/03/2023).

Fixada assim a ementa pelo TJSP, e sendo reconhecido o pertencimento da empresa de saúde e da instituição financeira ao mesmo grupo econômico, depreende-se que os dados de determinada pessoa foi transmitido sem o consentimento do correntista à empresa parceira.

A instituição destinatária dos dados, por sua vez, entabulou contrato e cobranças com base nos dados que indevidamente recolheu, o que resultou, claro, em litígio judicial. Adiante, se ampliada a pesquisa[21], o número passa para 64 (sessenta e quatro) processos, de 2014 até 2023, em panorama que não guarda indicativo com evento circunstancial, dado o número de contratos impugnados, a envolver as mesmas duas instituições e em anos distintos. Novamente, um cenário de coleta, uso e tratamento de dados indevidamente e que gerou litigiosidade a desaguar do Poder Judiciário, sem que a LGPD, seus instrumentos e órgãos correlatos, tenham auxiliado ou sido respeitados. Possivelmente, a regulação e manuseio do quanto possibilitado pela lei protetiva de dados pessoais ainda não é suficiente, havendo campo para que se colham frutos do quanto vivenciado em outros locais, especialmente no continente europeu, que guarda histórico pioneiro (ao menos na edição de diploma específico) e atuação

[21] Utilizados os termos “Bradesco”, “Odontoprev” e “descontos indevidos” (com uso do filtro “E”), no site www.tjsp.jus.br, em 28/08/2023.

mais acentuada, ou mesmo em casos análogos ocorridos no Brasil, objeto do próximo tópico.

2.2 Caso BMG e a decisão nº 13/2022 da Secretaria Nacional do Consumidor (SENACON). Caso PAN e o despacho nº 435/2021 da Secretaria Nacional do Consumidor (SENACON). Repercussão na litigiosidade.

Em agosto de 2022 foi amplamente noticiada na imprensa[22] a imposição de uma multa ao banco BMG pela Secretaria Nacional do Consumidor (SENACON) por uso indevido de dados de aposentados com conta na instituição. Segundo constou dos veículos de comunicação, a instituição se valeu de bancos de dados montados por correspondentes bancários, sem consentimento dos clientes, para oferta de empréstimos e cartões de crédito consignados a idosos. Em exame específico ao procedimento levado a efeito na SENACON, denota-se que o impulso inicial, e principal, ocorreu com a emissão da nota técnica 243/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ (Processo nº 08012.001478/2019-48)[23] em julho de 2019 (SENACON, 2019a), na qual constou como representante o Instituto Brasileiro de Defesa do Consumidor (Idec) e como representado o banco BMG, contendo a seguinte ementa:

> Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hipervulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.

Resumidamente, foram apresentadas denúncias de que a instituição financeira em comento se valeria de dados vazados de aposentados e pensionistas vinculados ao Instituto Nacional do Seguro Social (INSS) para realização de abordagens abusivas aos beneficiários, no fito de oferta e contratação de empréstimos e cartões de crédito consignados, o que estaria levando idosos a situação de superendividamento. Conforme relatado na nota, instado previamente a se manifestar, o INSS (acorde informação no bojo da nota técnica mencionada) explanou em maio de 2019 que o maior número de reclamações em sua ouvidoria dizia respeito

---

[22] Notícias consultadas em 30/08/2023: https://economia.uol.com.br/noticias/redacao/2022/08/03/bmg-e-condenado-a-pagar-multa-por-uso-indevido-de-dados-pessoais.htm; e https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2022/08/04/bmg-tera-que-pagar-multa-de-r-51-milhoes-por-oferta-abusiva-de-consignado.ghtml.

[23] Nota disponível em: https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/notas-tecnicas/anexos/nota-tecnica-243.pdf.

a operações de empréstimo consignado, cartão consignado e margem consignável das instituições financeiras. E que dentre as instituições com maior número de reclamações, o banco BMG estava em quarto lugar, sendo notificada a versada empresa em 23 de maio de 2019 para se manifestar, e negou os fatos. Solicitada também pesquisa junto ao Sistema Nacional de Informações de Defesa do Consumidor (SINDEC) quanto às práticas sob reclamo, foram localizados, no mesmo sentido, reclamos do banco relacionados a publicidade abusiva e crédito consignado.

Na fundamentação, apresentou-se indicativo de uso indevido de dados e abuso da vulnerabilidade de pessoas idosas, que não estariam compreendendo corretamente as abordagens efetuadas e, consequentemente, estariam também realizando contratos indesejados, e sugeriu-se a instauração de processo administrativo sancionador.

Em julho de 2021, foi então noticiada[24] a imposição, em primeiro grau administrativo, de multa de R$ 5,1 (cinco, vírgula, um) milhões de reais ao BMG (SENACON, 2019b).

A SENACON, ao impor a sanção, apontou a ocorrência de oferta abusiva e contratação de empréstimos consignados mediante utilização indevida de dados de consumidores idosos. Os dados, segundo consta, eram coletados por correspondentes bancários em tarefa de cadastro, sem qualquer aviso de que seriam usados para montagem de banco de dados, o que ocasionou a exploração da vulnerabilidade das pessoas mediante a oferta de dinheiro emprestado seguido de descontos nos benefícios. Em desfecho, em agosto de 2022 foi noticiado[25] o julgamento dos recursos (SENACON, 2019c), com manutenção da multa ao BMG, e afastamento da tese de lícita coleta de dados, porquanto, mediante atuação abusiva de seus correspondentes bancários, foi montado banco de dados sobre os idosos com benefícios sem o consentimento escrito deles, e sem escorreita fiscalização dos correspondentes pelo banco, que ao final se beneficiou dos dados[26].

Nesse cenário, nenhum aspecto regulatório da LGPD funcionou a contento, seja em âmbito fiscalizatório, informativo ou sancionador, subsistindo uma forma de atuação que, gerada por tempo suficiente, terminou por lesionar um sem número de pessoas. Menos ainda funcionaram mecanismos internos de autorregulação.

Adiante, para fins de exame da possível efetividade da sanção administrativa aplicada,

---

[24] Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-multa-banco-por-utilizar-dados-sem-consentimento-de-consumidores-idosos.

[25] Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/bmg-tera-que-pagar-multa-de-r-5-1-mi-por-oferta-abusiva-de-consignado.

[26] Inteiro teor da decisão disponível em: https://static.poder360.com.br/2022/08/Decisao-no-13_ASSESSORIA-SENACON_GAB-SENACON_SENACON-Decisao-no-13_ASSESSORIA-SENACON_GAB-SENACON_SENACON-DOU-Imprensa-Nacional.pdf.

com verificação da maior ou menor litigiosidade decorrente de contratos firmados em períodos anteriores e posteriores ao processo administrativo em estudo, efetivamos a análise de dados relacionados a processos direcionados ao banco BMG (na figura de réu), com questionamento de contratos, no decorrer de determinado período e em uma comarca específica do interior do Estado de São Paulo.

A pesquisa foi realizada na comarca de Estrela d'Oeste/SP, abarcando-se processos distribuídos na Vara Cível e no anexo de Juizado Especial Cível do mesmo foro, por ocasião da proximidade física da residência e local de trabalho do pesquisador, bem como porque inviável a análise de impacto na litigiosidade em todo o estado de São Paulo e, menos ainda, em todo o país.

A escolha de pesquisa em uma única comarca é facilitada, ademais, porque é necessário que se verifique ao menos o ano do contrato sob litígio, o que se torna praticamente impossível caso empreendida a apuração em base territorial maior. Igualmente, não foram separados apenas os casos em que idosos eram componentes do polo ativo, sendo o objetivo a verificação da influência da multa na litigiosidade referente ao banco multado. E, nessa tarefa, após coleta de dados (anexos 1 e 2), verificou-se o seguinte.

Consoante o critério do ano inicial de vigência do contrato questionado, foi averiguado que: 3 (três) contratos com vigência em 2013 foram questionados perante a Justiça; 2 (dois) contratos com vigência em 2014 foram questionados; 49 (quarenta e nove) contratos com vigência a partir de 2015 foram questionados; 25 (vinte e cinco) contratos com vigência a partir de 2016 foram questionados; 06 (seis) processos com ano inicial de vigência em 2017 foram questionados; 2 (dois) processos com ano inicial de vigência em 2018 foram questionados; 03 (três) processos com ano inicial de vigência em 2019 foram questionados; 4 (quatro) com ano inicial em 2020 foram questionados; 11 (onze) contratos com ano inicial de vigência em 2021 foram questionados; 5 (cinco) contratos com ano inicial de vigência em 2022 foram questionados; e 2 (dois) contratos com ano inicial de vigência em 2023 foram questionados[27].

Nesse primeiro recorte, relativo ao ano de vigência inicial dos contratos postos sob litígio em face do banco BMG, denota-se que o ápice da litigância ocorreu em 2015 (49 contratos), seguindo-se de razoável diminuição em 2016 (25 contratos) e arrefecimento mais incisivo a partir de 2017 (6 contratos). Houve ligeiro aumento da litigância relativa aos

[27] Pesquisa realizada entre os dias 21/08/2023 a 25/08/2023 no sistema de automação judicial (SAJ) relacionado ao TJSP.

contratos com início em 2021 (11 contratos), mas sem aumento substancial, haja vista que em 2022 apenas 5 contratos foram postos sob debate na Justiça. Assim sendo, se não foi nítido o impacto do início do procedimento administrativo perante a SENACON, que se deu em 2019, ao menos não houve crescimento significativo da litigiosidade dos contratos firmados após 2015, não havendo de se excluir, por completo, a influência do procedimento e da multa nas ofertas mais justas aos cidadãos e no resultado de contratos menos atacados pelos cidadãos.

Segundo o critério do ano do processo (e não do ano inicial de vigência do contrato debatido no processo), foram encontrados os seguintes dados: em 2015 foram distribuídos 8 (oito) processos em face do BMG; em 2016 foram distribuídos 6 (seis); em 2017 foram distribuídos 13 (treze); em 2018 foram distribuídos 37 (trinta e sete) processos; em 2019 foram distribuídos 10 (dez) processos; em 2020 foram distribuídos 2 (dois) processos; em 2021 foram distribuídos 11 (onze) processos; em 2022 foram distribuídos 5 (cinco) processos; e em 2023 foram distribuídos 2 (dois processos)[28]. Aqui os números apresentam dados mais significativos, pois o auge da distribuição de processos foi em 2018, ano anterior ao início efetivo da fiscalização da SENACON em relação ao BMG. Em 2019 o número de processos caiu de 37 para 10, com ligeira subida em 2021 (11 processos) mas sem aumento significativo depois de 2018.

Enfim, a litigiosidade foi incisivamente menor após o início das fiscalizações pertinentes ao procedimento sancionador da SENACON em 2019, havendo de se pontuar pela coerente possibilidade de que o banco tenha adotado medidas preventivas e de conciliação extrajudicial antes que a celeuma se transformasse em processo judicial. Portanto, se os dados não confirmam em absoluto que as práticas indevidas do banco cessaram, ao menos demonstram que a litigiosidade em relação a ele não aumentou, o que é sinal de menor índice de insatisfação dos consumidores com as práticas da instituição financeira. Um cenário, nesses moldes, que indica que uma regulação mais detalhada e acessível, a ponto de tornar apta a identificação e repressão de fenômenos e comportamentos contrários à LGPD quanto antes, pode auxiliar na diminuição da litigiosidade.

Em pesquisa com metodologia semelhante, e agora relacionada ao banco PAN S.A., depreende-se que, conforme publicação no diário oficial da União de 31/05/2021[29], a SENACON aplicou multa de R$ 8.000.000,00 (oito milhões de reais) à instituição

[28] Pesquisa realizada entre os dias 21/08/2023 a 25/08/2023 no sistema de automação judicial (SAJ) relacionado ao TJSP.

[29] PROCESSO ADMINISTRATIVO Nº 08012.001462/2019-35; DESPACHO Nº 435/2021; SECRETARIA NACIONAL DO CONSUMIDOR; DIÁRIO OFICIAL DA UNIÃO DE 31/05/2021.

(SENACON, 2019e), em acolhimento à nota técnica nº "35/2021/CSASENACON/CGCTSA/DPDC/SENACON/MJ (14657462)" (SENACON, 2019d). Referida nota técnica[30] apontou em ementa (pg. 1 da nota):

> Conduta abusiva na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem nociva por telefone de idosos aposentados e pensionistas do INSS. Exploração da hipervulnerabilidade do idoso. Práticas abusivas na oferta de empréstimos consignados: ausência de informação clara e adequada e violação de dados pessoais de idosos.

Segundo consta, e em panorama análogo ao do banco BMG, foi constatado pelo Instituto de Defesa Coletiva e apresentado à SENACON que, mediante vazamento de dados de aposentados e pensionistas vinculados ao INSS, foram realizadas abordagens abusivas a consumidores idosos, para fins de obtenção de empréstimos ou cartões de crédito, antes mesmo do recebimento de um primeiro benefício. Em uma das informações constantes da nota técnica e afirmadas com base em depoimentos, apontou-se que, sem consentimento, por volta de setembro de 2018 um correspondente do banco afirmou que "comprava dados de potenciais clientes (pessoas aposentadas, pensionistas, ou, ainda, pessoas que se encontram em idade próxima à mínima exigida para recebimento de benefícios previdenciários)", por intermédio de terceiros, e que também "abria cadastro e bancos de dados de potenciais clientes sem qualquer política de privacidade e sem qualquer informação ao consumidor" (pg. 12 da nota). Além disso, o correspondente do banco PAN afirmou efetuava disparos de SMS, sem conhecimento dos dados dos destinatários, em uma média de 3.600.000 (três milhões e seiscentos) mil disparos por ano, em postura deveras agressiva. Houve, ainda, a constatação de que o banco se utilizava de dados obtidos com parceiros. Posteriormente, conforme adiantado, houve reconhecimento de violação aos direitos do consumidor, com imposição de multa com decisão publicada em 31/05/2021.

A análise da influência da multa na litigiosidade dos contratos efetuados com o banco PAN na comarca de Estrela d'Oeste (base de dados de mais eficaz alcance do subscritor), e realizada no período de 05/09/2023 a 06/09/2023 (anexo 3), indicou que houve queda considerável de contratos questionados a partir de 2021, considerando o ano de assinatura do contrato. De 12 (doze) contratos assinados em 2020 e questionados perante a 1ª Vara de Estrela d'Oeste, caiu o número para 2 (dois), considerando os contratos assinados em 2021 e questionados na Justiça. Quanto aos contratos assinados em 2022, o número foi de 5 (cinco)

[30] Disponível em: https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/notas-tecnicas/anexos/114977575_Nota_Tecnica_n__35.pdf/view .

questionados, e nenhum dentre os assinados em 2023. Quanto ao número de ações distribuídas nos anos em face do banco PAN, os números caíram a partir de 2021. Foram ajuizadas contra o banco PAN em 2021 um total de 10 (dez) ações questionando contratos. Em 2022 o número caiu para 7 (sete), e em 2023 o número (à data da pesquisa) era de 3 (três) ações.

Deixa-se de mencionar os dados colhidos no Juizado Especial Cível da mesma comarca em razão do extremado baixo número (apenas 6 de 2016 a 2022), tornando nebulosa qualquer conclusão. Portanto, há indicativo mínimo de mudança de procedimento da empresa após a atuação administrativa, afinal se o número de contratos assinados de 2021 em diante diminuiu, é porque possivelmente a postura agressiva foi arrefecida, ainda que minimamente. E se o número de processos também diminuiu, há indicativo possível de maior proatividade no amparo aos direitos do cidadão antes que os problemas fossem apresentados à Justiça. Em comparativo com a experiência europeia, conquanto dificultoso seja a pesquisa de diminuição ou não de litígios judiciais lá existentes (considerando que são inúmeros os países que compõem a União Europeia), é possível verificar que (tema dos próximos tópicos), no mínimo, naquele ambiente que inspirou a nossa legislação há regulação estatuída de forma mais democrática, clara e eficiente, o que de fato pode auxiliar em nossa realidade, dado que o pouco feito aqui já apresentou resultados, ainda que não tão significativos até o momento.

2.3 Comparação com a experiência europeia

Dezem e De Lucca (2018), em artigo publicado no mesmo ano de promulgação da LGPD, avaliaram os sistemas europeu e estadunidense de proteção de dados como possíveis modelos aptos a gerarem lições para o Brasil. Muito embora a temática protetiva das informações pessoais provenientes de dados não seja em si uma pauta nova, o ambiente no qual a coleta, armazenamento e uso desses dados ocorrem, em meio ao avanço da tecnologia e a uma sociedade com as informações e o conhecimento como ativos de grande valor, as soluções devem ser novas e coerentes, com o fim de que com novos avanços melhor se tutele o indivíduo por meio da proteção de seus dados.

De início, como também abordado no capítulo primeiro, no que toca ao percurso empreendido em solo europeu, tem-se que a legislação do versado continente para a regulação de dados, denominada “General Data Protection Regulation” (GDPR), data de 2016 e detém vigência desde 25 de maio de 2018. Segundo informações de sítio eletrônico relacionado ao

histórico da lei em comento[31] e da própria tutela da privacidade no continente, em 1995 foi aprovada a Diretiva 46 do Parlamento Europeu e do Conselho[32] para proteção de dados na Europa, com previsão de standards mínimos de segurança para a privacidade dos dados, a partir dos quais os países estipularam suas legislações específicas. Concomitantemente, a internet incrementou significativamente os potenciais de extração e tratamento de dados. A partir dos anos 2000, a maioria das instituições financeiras passou a oferecer serviços online. Na sequência, Facebook e Google abrangeram suas operações ao público, com grande potencial de acesso a dados pessoais. Em 2002, o Parlamento Europeu e o Conselho aprovaram a Diretiva 58[33], relativa ao tratamento dos dados pessoais e à proteção da privacidade no contxto das comunicações eletrônicas, de modo a reforçar a Diretiva 46 (DEZEM e DE LUCCA, 2018), conhecida como "ePrivacy Directive". Cíntia Rosa Pereira de Lima (2015 apud DEZEM e DE LUCCA, 2018, pg. 15), assim comenta o considerando número 9 dessa diretiva:

> A *ePrivacy Directive* foi uma resposta à economia informacional acima destacada, na medida em que impõe limites à coleta, armazenamento e utilização de dados pessoais no contexto das comunicações eletrônicas, independentemente da tecnologia utilizada. Assim, essa Diretiva traz como seu objetivo principal reduzir ao mínimo o tratamento de dados pessoais e de utilizar, quando necessário, mecanismos que assegurem o anonimato do usuário (Considerando 9).

Ao final, em 2011, após ser acusada de indevida vigilância de e-mails, a Autoridade Europeia para Proteção de Dados declarou que a União Europeia precisava de uma abordagem mais abrangente sobre a proteção dos dados pessoais, em avanço à diretiva criada em 1995, como resposta às inovações tecnológicas (DEZEM e DE LUCCA, 2018).

No ano de 2016 o GDPR foi aprovado. Nesse passo, Dezem e De Lucca (2018) apontam que o modelo europeu adota solução regulatória com origem em Diretivas e deságue na GDPR, em estipulação de regramento geral e básico relativo à proteção de dados válido para os países componentes do bloco.

O modelo estadunidense, em outro vértice, adota solução eminentemente autorregulatória pelo setor privado, sem lei específica e geral sobre o tema, ao passo que os estados da federação americana adotam método de regulação setorial, com atenção aos dados

[31] Disponível em: https://gdpr.eu/what-is-gdpr/.
[32] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&qid=1692060003555.
[33] Disponível em: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf

relacionados especificamente a setores como saúde, crédito e ensino (DEZEM; DE LUCCA, 2018).

A solução europeia é, assim e em certo aspecto, útil ao exame da problemática brasileira, afinal a LGPD é também originada de um ente central (Poder Legislativo Federal), com previsões genéricas e aplicabilidade a todos os estados da federação e áreas de atuação econômica.

Nesse mesmo sentido, De Lucca e Maciel (2019), ao ressaltar a influência da legislação europeia sobre as outras leis do mundo, apontam que "o fato é que não terá sido diferente em matéria de proteção de dados pessoais, na qual a nossa LGPD, como se sabe, foi plasmada, na maioria, à imagem e semelhança do RGPD da União Europeia" (DE LUCCA; MACIEL, 2019, p. 30).

Portanto, sem que se intente fixar eventual superioridade de um modelo sobre outro, a experiência da Europa no tratamento de dados há de ser pesquisada como possível paradigma para atuação de empresas brasileiras na coleta, armazenamento e uso de dados, a fim de que o modelo europeu e o espírito das reflexões e conclusões lá tiradas possa ser levado a efeito também no Brasil, ou ao menos ser considerado para atuação mais aproximada à práxis lá efetivada. Para tanto, e considerando os limites do estudo, serão primeiramente destacas algumas decisões tomadas naquele continente pelas autoridades lá atuantes.

2.4 Uso indevido de dados e processos administrativos na Europa

Ao menos desde 2009, mediante a Diretiva 136[34], o Parlamento Europeu e o Conselho exigem o consentimento expresso do indivíduo para o armazenamento das informações, com detalhamento mínimo acerca de suas características, a incluir o seu caráter prévio e clareza, acrescentando o direito de retirá-lo quando de sua intenção. Ou seja, muitos anos antes da aprovação do GDPR, na Europa já se dissertava acerca da problemática do consentimento no contexto de intenso fluxo de informações, sendo necessário então que se analisem algumas das decisões atuais, já sob a luz da legislação vigente (GDPR).

Para tanto, por melhor organização e seleção de materiais, haja vista a inviabilidade de pesquisa de decisões em todas as autoridades nacionais de proteção de dados de todos os países europeus vinculados à GDPR, foi realizada pesquisa a partir de um site específico e especializado na identificação de más práticas empreendidas por empresas em prejuízo dos

[34] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0136

cidadãos, denominado *deceptive patterns* (no sentido de padrões enganadores ou ardilosos).

No referido site há link específico[35] com destaque de casos em que empresas foram sancionadas por órgãos regulares de seus países, principalmente relacionados a proteção de dados, em razão de uso de padrões de comportamento que lesam indivíduos e que os levam a fazer o que em realidade não desejam. Dentre todos os casos ali mencionados, selecionamos alguns, principalmente os provenientes da Agência Espanhola de Proteção de Dados em razão da didática e clareza dos argumentos, para fins de exame da resposta dada pelas autoridades a atos de empresas de variados ramos que guardam mínima semelhança com atos que podem ser praticados também no Brasil.

No "Procedimiento Nº: PS/00332/2020"[36] a Agência Espanhola de Proteção de Dados (AEPD) condenou uma empresa a pagar uma multa de 8.000 (oito mil) euros por uso indevido de dados de um cliente para fins de envio de publicidade. Ao que consta, após adquirir um veículo de determinada sociedade empresária, o reclamante passou a receber publicidade via e-mail, e apresentou reclamo junto à Agência Espanhola de Proteção de Dados (AEPD). Mediante uma primeira intervenção do competente órgão, a empresa interpelada se comprometeu a suprimir os dados do cliente de seus cadastros, e não mais enviar os materiais publicitários. No entanto, mesmo após essa intercessão, a empresa iniciou o envio ao mesmo cliente de mensagens via SMS ao seu telefone celular, com fins comerciais, o que deu ensejo à instauração de procedimento sancionador. Segundo o examinado, ao invés de cessar a conduta, a instituição empresarial apenas diminuiu a frequência do envio de comunicações ao antigo cliente, por mais que ele pleiteasse baixa para não mais ser comunicado de ofertas e publicidades.

No caso, a AEPD pontuou pela existência no sítio eletrônico da reclamada de banner com informações sobre coleta e tratamento de dados do usuário, sem que fosse dada a opção de negativa àquela hipótese de tratamento. Nestes termos, mediante uma única opção de botão, o cliente passava a concordar que os dados dele seriam usados para fins como recebimento de informações sobre produtos e serviço, com aceitação simples a uma "declaração de consentimento". O conteúdo da referida declaração, por sua vez, era acessada por um link específico, com previsão genérica de permissão para que os dados do usuário fossem usados para marketing personalizado e estudos de mercado pela empresa controladora.

Além desse conteúdo, ainda eram previstas como "finalidade" o envio de convites para

[35] Disponível em: https://www.deceptive.design/cases (Endereço copiado em 02/09/2023).
[36] Decisão disponível em: https://www.aepd.es/es/documento/ps-00332-2020.pdf

eventos, informações diversas sobre veículos, ofertas de veículos novos, ofertas de financiamentos, dentre outros. Os destinatários desses dados, outrossim, não seriam apenas a empresa controladora, mas também outros parceiros comerciais que também poderiam enviar ofertas e "experiência". Os dados requeridos na relação, enfim, eram nome, sobrenome, endereço e detalhes para contato, como e-mail, telefone e código postal.

Em argumentação, a empresa afirmou, como um dos argumentos para renitência no envio de publicidade por distintos meios, que após o cliente entrar em contato para informar sobre nova a reclamação, acabou por aceitar novamente a política de privacidade e declarar consentimento sobre uso de dados. Em outras palavras, a empresa, ao admitir "protocolo" de reclamação sobre uso indevido de dados de usuário, de certa forma impôs a ele novamente a aposição de concordância com suas práticas. Ao mencionar legislação sobre comércio eletrônico, a AEPD fixou ser proibido o envio de comunicações publicitárias ou promocionais por correio eletrônico, ou outro meio equivalente sem prévia solicitação, ou autorização expressa do destinatário. Ainda, pontuou a entidade que mesmo em caso de previsão contratual para tais comunicações, deve ser sempre oferecida ao usuário a possibilidade de se opor ao tratamento de dados oferecido em procedimento simples e gratuito a todo o instante, desde o momento de coleta das informações até as comunicações posteriores.

Nesse sentido e em exemplo, a autoridade de proteção informou que se as comunicações forem enviadas por correio eletrônico, o meio de se oferecer a recusa à continuidade do envio deve ser necessariamente incluído na mesma ocasião, como um link por meio do qual esse direito possa ser exercido. Quanto à exigência de informações e preenchimento de formulários para permissão do próprio contato com a empresa, dispôs a autoridade que é ilícita a reiterada condição de aceitação da política de privacidade e a declaração de consentimento para uso de dados, pois invariavelmente tal procedimento ocasionará, em círculo vicioso, nova rodada de envio de publicidade indevida ao cliente, com mais envios por mais que ele reclame dos mesmos envios, em comportamento contrário ao artigo 6.1 da GPDR. O referido artigo, em tempo, estabelece que o tratamento de dados será lícito somente se atendidas as hipóteses ali previstas, dentre elas a de que a coleta de dados será limitada até a extensão necessária para a execução do contrato, ou no limite das medidas requeridas pelo próprio titular dos dados. Assim sendo, para qualquer outro tipo de tratamento ou comunicação, como na hipótese de receber ofertas e ser objeto de marketing personalizado, haverá de se obter consentimento para esses fins específicos.

Relativamente à obtenção genérica de consentimento, a autoridade, mencionando o art. 7º da GDPR, pontuou que o consentimento em si deve obedecer a condições.

Nesse contexto: i) a prova de consentimento obtido remanesce ao encargo do controlador; ii) se o consentimento for proferido em documento que contenha outras informações, deve ele ser claramente destacado dos outros temas, de forma inteligível, clara, simples e de fácil acesso; iii) o titular pode retirar seu consentimento a qualquer momento; iv) antes do consentimento deve existir a informação, e o modo de retirada do consentimento deve ser tão fácil quanto o modo de sua colheita; e v) na avaliação da validade do consentimento, deve ser considerada a exigência de obtenção dos dados para finalidades não necessárias ao cumprimento do contrato. Outrossim, aponta o considerando 32 do art. 7º da GDPR que o consentimento de ser proferido por ato afirmativo claro, e de maneira livre, específica, informada e inequívoca do titular quanto à aquiescência sobre o tratamento de seus dados, sugerindo-se declaração por escrito ou oral, permitindo-se marcação de uma "caixa" quando da visitação de um sítio eletrônico. Lado outro, segundo o mesmo considerando, o silêncio, opções pré-marcadas, ou mesmo a inércia não devem ser tomados por consentimento válido. Se várias forem as finalidades do tratamento, o consentimento deverá ser efetuado para todas elas e, por fim, se o consentimento for dado após requisição por meio eletrônico, não deverá ser ele – consentimento – causa de perturbação do serviço para o qual ele é destinado.

Ao final da fundamentação, conclui a AEPD, em sentido semelhante ao que é previsto no art. 7º, LGPD, que o tratamento de dados em hipótese distinta da relativa à necessidade para execução do contrato em si, especialmente no que tange às mensagens de publicidade e oferta, exige para sua licitude o específico consentimento, com todos os caracteres de sua validade conforme art. 8º, a exemplo da formalidade da expressão (por escrito ou meio que o demonstre), existência de cláusula destacada, clareza, facilidade de revogação, dentre outros.

A multa terminou fixada em razão do envio de publicidade sem consentimento, e por requisição de dados para finalidade distinta da almejada pelo titular (caso de exigência de dados e declaração de consentimento para efetuar reclamação perante a empresa).

Em outra decisão de relevo da mesma AEPD, emanada no "Expediente Nº: PS/00226/2020"[37], foi aplicada uma multa a uma instituição financeira por condicionar o consentimento de correntistas ao tratamento de seus dados pessoais à isenção de tarifa. Segundo sete clientes do banco que apresentaram reclamação à agência, era-lhes exigido que aceitassem os tratamentos de dados pessoais indicados e previamente marcados/escolhidos.

Do contrário, era imposta uma tarifa de cinco euros por mês para manter a conta. Dados relacionados à identificação, meios de contato, estado civil, número de filhos, data e local de

[37] Disponível em: https://www.aepd.es/es/documento/ps-00226-2020.pdf

nascimento, nacionalidade e dados profissionais eram exigidos, acompanhados da informação genérica de que seriam tratados segundo as informações básicas de proteção de dados que deveria ser lida pelo cliente. No que tange a essas informações a serem lidas, após genérica menção à legitimação de carácter geral para tratamento de dados e dos direitos dos titulares, solicitava-se o consentimento para uma série de finalidades, com opção de sim ou não: consentimento para envio de publicações comerciais personalizadas por qualquer canal, e sobre praticamente qualquer serviço prestado pelo banco (empréstimos, seguros, financiamentos, descontos, entre outros), acorde os dados do correntista e os produtos/serviços por ele adquiridos; consentimento para consulta dos dados do correntista relacionados à sua solvência, para ofertas de produtos personalizados; e consentimento para envio e compartilhamento de seus dados a terceiros componentes do grupo econômico. Ao final, apenas se lograria a conclusão de um "perfil digital" caso tais aquiescências quanto aos dados ocorresse. E somente com a criação desse perfil é que não seriam cobradas tarifas de adesão e de "manutenção" ou administração dos correntistas que usassem cartões de débito, mediante constante verificação de cumprimento.

O banco, a seu turno, alegou que a tarifa era necessária à prestação dos serviços bancários, sendo elemento essencial do contrato, e que colheu o consentimento.

A AEPD pontuou que a vinculação de uma isenção à obtenção de dados pessoais prejudica o caráter de liberdade do consentimento em prejuízo aos titulares dos dados, e em procedimento que não se equivale a um programa de fidelidade.

Em especial, citou a agência espanhola o item 4 do art. 7º da GDPR, que pontua que para avaliação da liberdade do consentimento é necessário que se verifique o contexto em que ele foi proferido:

> *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*[38].

Nesses termos, se a execução de um contrato ou a prestação de um serviço são condicionados ao consentimento para tratamento de dados não estritamente necessários, há sérios indicativos de agravo à liberdade, afinal, da ausência de consentimento resulta claro

[38] "Ao avaliar se o consentimento foi dado livremente, deve-se considerar principalmente se, entre outras coisas, a execução de um contrato, incluindo a prestação de um serviço, está condicionada ao consentimento para o processamento de dados pessoais que não são necessários para a execução desse contrato."

prejuízo financeiro ao titular.

Aliás, segundo o considerando (mencionado como "recital", ao lado dos artigos em si do diploma) 43 da GDPR a coleta de dados é inválida para a execução de contratos se não há indicativo de incremento ou melhoria no desempenho. E, no caso, nada indica que o serviço bancário em si se tornaria melhor, mas apenas que mais ofertas sobre novos e distintos produtos e serviços seriam constantemente oferecidos.

Em hipótese semelhante, a Corte de Justiça da Europa[39] considerou inválida a atitude de empresa de apostas que vinculou a possibilidade de jogo ao recebimento de publicidade de terceiros (uma forma de se manipular o consentimento, permitindo-se uso de dados desconhecidamente pelo usuário).

Ainda no que toca à instituição bancária em comento, relativamente a um determinado período e alguns clientes, pontuou o órgão que a entidade violou o item 1 do art. 6º, da GDPR, ao previamente marcar "caixas" de opções para tratamento de dados, delegando-se ainda o consentimento para opções de aceitação designadas como "eu aceito" ou "eu concordo".

Além disso, o considerando número 32 da GDPR ("recital" 32) aponta que caixas pré-marcadas não devem ser aptas a traduzir consentimento. Nesse mesmo contexto, a Autoridade Nacional de Supervisão para o Processamento de Dados Pessoais da Romênia, no "case c-61-19"[40], também fixou que a simples inatividade ou o uso de caixas pré-marcadas não conduzem à conclusão pelo consentimento válido, considerando praticamente impossível a verificação objetiva da liberdade do cidadão que não desmarca uma opção já feita por ele, sendo crível e possível que ele não tenha lido ou notado tal opção (a mesma condenação foi proferida pela agência de proteção de dados espanhola ao oferecer a um hospital, caixas pré-marcadas para oferta de publicidade[41]).

A mistura de propósitos em um único "feixe" de opção também já foi avaliada por cortes europeias de proteção de dados como ilegal. Em outras palavras, a referida conduta significa incluir uma série de finalidades de tratamento em uma única opção (ou botão), sem que para cada finalidade de tratamento haja uma única opção (ou botão) específicos, a se incrementar a ciência e a liberdade no consentimento. Também pode significar a inclusão da hipótese de tratamento conjuntamente a outra questão contratual que não tem relação com dados, tudo pela

[39] Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7790677

[40] Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=233544&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=13705373

[41] Disponível em: https://www.aepd.es/es/documento/ps-00204-2022.pdf

mesma “opção” ou “botão”.

A Agência Espanhola de Proteção de Dados, no “Procedimiento Nº: PS/00234/2020”[42], considerou ilegal a conduta de uma plataforma de divulgação de cursos que, concomitantemente ao preenchimento de um questionário e como condição necessária de acesso ao serviço, exigia a aceitação de uma política de privacidade que compreendia uma série de hipóteses distintas de tratamento de dados pessoais, para além do necessário, como inclusão do usuário em programas de prospecção comercial, ofertas, publicidade, envio de conteúdos editoriais, segmentação de envios segundo o perfil, entre outros, apontando ao final que a negativa a esses tratamentos deveria ser comunicada via carta ou e-mail.

Na mesma oportunidade em que deveria aceitar a política de privacidade para obter informações sobre cursos, não se identificava o responsável pelo tratamento e nem os meios de o contatar, o que prejudicava o exercício e reclamo dos direitos, em confronto ao art. 13, GDPR, que leciona que no instante de colheita dos dados todas essas informações devem ser fornecidas (incluindo-se explicações sobre a necessidade e propósito da colheita).

Além disso, o art. 6º, GDPR, impõe que o consentimento deve ser conferido para fins específicos, e não implícitos em um corpo de medidas anunciadas.

A mesma conclusão foi tirada pela agência espanhola em caso análogo no qual não foram separadas as obtenções de consentimento para fins puramente comerciais e para acesso a funcionalidades de busca de emprego[43]. O uso de mesmos botões ou opções para múltiplos casos que dependam de consentimento, ou a oferta de caixas pré-marcadas ou preenchidas, são práticas apenas pelas autoridades europeias em casos não isolados, todas com fundamento na retirada de liberdade do usuário.

Em outra hipótese identificada como contrária à legislação protetiva de dados[44], a autoridade francesa competente para análise de dados multou uma empresa relacionada aos serviços de telefonia celular por impor o envio de anúncios personalizados aos clientes por meio de um aplicativo após uma atualização de seus sistemas operacionais, sem prévio consentimento.

Além disso, em caso de contrariedade ao envio dos anúncios, impôs a obrigatoriedade de implemento de uma série de etapas para mudança da configuração, dificultando o exercício de direitos. Concluiu assim o órgão que a atualização impunha uma configuração padrão sem espaço para questionamento do consentimento, exigindo-se, lado outro, intensa atuação do

[42] Disponível em: https://www.aepd.es/es/documento/ps-00234-2020.pdf
[43] Disponível em: https://www.aepd.es/es/documento/ps-00110-2020.pdf
[44] Disponível em: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046907077

mesmo usuário para desativação.

Semelhante posicionamento foi tomado pela autoridade polonesa de proteção de dados, em especial no caso de uma empresa que impedia a retirada de consentimento de seus clientes para tratamento de dados ou mesmo a exclusão de seus dados[45].

Nesse sentido, o art. 25, GDPR, com título "data protection by design and by default", prevê que no momento da organização do processamento de dados o controlador deverá, durante a própria atividade de "montagem" de uma atividade que demande dados, implementar medidas e técnicas que de antemão já sejam direcionadas à proteção dos dados (pseudonimização, minimização de dados, em exemplo), se possível com adoção de certificação, utilizando-se apenas do necessário ao serviço. E não o contrário, com estipulação de técnicas que diminuam a vigilância e o consentimento dos clientes sobre o manejo de seus dados e, claro, em última análise de sua liberdade, razão da imposição da sanção no caso.

A Autoridade Dinarmaquesa para proteção de dados, a seu turno, em decisão que reconheceu algumas práticas nocivas às leis sobre dados pessoais[46], enfrentou um caso em que uma empresa detinha como prática o oferecimento de três hipóteses de consentimento sobre a extensão de tratamento de dados: somente o necessário; personalizar configurações e aceitar tudo. Entretanto, os usuários do site da empresa que optaram pela aceitação total não receberam informações suficientes sobre todas as finalidades do processamento, pois tais esclarecimentos somente eram apresentados em uma segunda etapa, e após a conferência do "aceite". Tal metodologia não foi reconhecida como um consentimento informado, ainda que possível posteriormente a personalização e mudança de configurações, pois o art. 4º, inciso 11, GDPR, aponta que o consentimento apenas pode ser validamente considerado se for livre, específico, bem informado e sem ambiguidade. Além disso, considerou a autoridade dinamarquesa que o uso de cores distintas, no caso, prejudicou a liberdade de escolha dos usuários. Muito embora o uso de layout e design sejam de escolha da empresa, a utilização de cores de forma análoga a um semáforo foi identificada como abusiva e não bem informada, pois a escolha de aceitação total era apresentada com coloração verde, em conduta não transparente, conforme exige o art. 5ª, inciso 1, GDPR. Inscrições forçadas em "sorteios" após coleta de dados por sites de notícias, como se de algo positivo ou de vantagem se tratasse, também foi considerando ilícito pela autoridade húngara de proteção de dados[47], ou seja, sem

[45] Disponível em: https://uodo.gov.pl/decyzje/ZSPR.421.7.2019

[46] Disponível em: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/okt/alvorlig-kritik-af-jppolitikens-samtykkeloesning-paa-wwwebdk

[47] Disponível em: file:///C:/Users/mluca/Downloads/NAIH-7058-5-2022-hatarozat%20(1).pdf

consentimento para propósito específico e sem necessidade para a prestação principal.

2.5 A utilização de cookies e suas limitações e os *dark patterns* fixados pela EDPB

Cookies são arquivos de internet que são aptos a armazenar, ainda que temporariamente, as informações relacionadas a um usuário que acessa determinada rede (AGRA e BARBOZA; 2019). De certa forma, eles permitem uma navegação mais "personalizada", pois dispensam a reiteração da prestação de informações já coletadas quando de novo ingresso no mesmo ambiente virtual, a exemplo de um login e senha. Tamanha é a relevância deste instrumento, que o uso em comum por uma determinada coletividade de empresas para fins de rastreamento (e direcionamento) de um consumidor quando da visita de qualquer dos sites do grupo é prática nociva denominada *spyware* (AGRA e BARBOZA; 2019). Em didático conceito, que abrange ilustração acerca do potencial desse instrumento, apontam LAUREANO e CORDELLI (2017; p. 52) que cookies:

> São arquivos trocados entre o navegador e o servidor web para uso on-line, os quais podem ser utilizados para autenticação, controle de sessão e definição de preferências ou de conteúdo do carrinho de compras de um site. Por exemplo, um cookie pode armazenar a ID de login do e-mail de um usuário; assim, ele não precisa efetuar login na página a cada nova visita. Alguns cookies são temporários e outros podem permanecer no disco rígido, sendo reutilizados ao visitar novamente determinado site. Os cookies também ajudam na coleta de informações (preferências) dos usuários sem o seu consentimento. Mesmo que o usuário navegue de forma anônima (sem se identificar), é possível coletar algumas informações por meio dos cookies de navegação (e o endereço IP identifica a origem do usuário).

Não sem surpresa, dado o potencial de coleta de informações, o uso de tais arquivos também foi objeto de debates nas cortes de dados europeias, especialmente no que tange à devida informação[48] e consentimento prévios ao implemento desse instrumento. A corte dinamarquesa de proteção de dados[49], nesse sentido, sancionou empresas que se utilizaram de cookies em seu site sem prévio consentimento válido dos titulares daqueles dados. Ainda, pontuou que as configurações utilizadas tornavam difícil a tarefa de rejeitar o uso de cookies, ao contrário dos comandos de aceitação, que eram de fácil manejo. Ou seja, em primeiro apontamento, se esse instrumento é apto a coletar dados, deve haver prévia permissão do

[48] Disponível em: https://www.aepd.es/es/documento/ps-00234-2020.pdf

[49] Disponível em: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/okt/alvorlig-kritik-af-alstroem-din-isenkraemmer-aps%E2%80%99-behandling-af-personoplysninger-om-hjemmesidebesoegende

titular, em acordo ao art. 6º, GDPR. Além disso, por mais que haja a opção de aceitação prévia do uso de cookies, garantindo-se o prévio consentimento, já decidiu a corte espanhola de dados[50] que a opção simples de rejeição completa do uso de cookies deve, concomitantemente, estar disponível ao visitante do site. O órgão francês responsável pela proteção de dados, em caso específico, aplicou pena a uma empresa por não permitir, efetivamente, que o uso de cookies fosse rejeitado, muito embora, de forma contraditória, informasse o visitante do direito de os rejeitar[51]. Não só o impedimento à recusa, mas também a imposição de dificuldades de desinstalar os cookies utilizados pelo site foi uma prática apontada como ilícita pela corte espanhola[52].

Em maior detalhamento sobre o conteúdo das informações devidas acerca do uso de cookies, a mesma corte espanhola de dados pontuou que a empresa responsável pela prática deve identificar o uso, mencionar os recursos a que deseja acesso por intermédio do implemento dessa ferramenta, o tempo de duração dos cookies e, claro, a fácil opção para recusá-los, considerando ao final o site da empresa como inseguro[53]. Até mesmo a exigência de várias etapas para a rejeição de cookies, ao invés da disponibilização de "botão" de rejeição completa e simples, foi apenada pelas autoridades europeias. Em interessante caso, a autoridade belga para proteção de dados[54] declarou ilícito o procedimento de determinada empresa que, sob o pretexto de permitir "navegação adicional", exigiu aceitação do uso de cookies, em procedimento que violou a liberdade no consentimento, violando o art. 4º, XI, e 7º, I, GDPR. Por último, a permissão de uso de cookies por parceiros foi considerada ilegal se, ao mesmo tempo, não é possibilitada no site a chance de recusa[55].

Além de do possível uso de cookies como instrumento de coleta subreptícia de dados pessoais, o Comitê Europeu para Proteção de Dados (European Data Protection Board – EDPB), organização de cúpula que reúne as autoridades nacionais de proteção de dados dos países europeus e a própria autoridade europeia para proteção de dados e que visa a aplicação informe e coerente da GDPR, em tarefa de construção de diretrizes e recomendações para melhores práticas, estatuiu uma gama de padrões denominados como "obscuros" (dark patterns) e indevidos se utilizados em plataformas de mídias sociais para coleta de dados. Em

[50] Disponível em: https://www.aepd.es/es/documento/ps-00264-2020.pdf
[51] Disponível em: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043867129
[52] https://www.aepd.es/es/documento/ps-00473-2019.pdf
[53] Disponível em: https://www.aepd.es/es/documento/ps-00185-2020.pdf
[54] Disponível em: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-103-2022.pdf
[55] Disponível em: https://www.aepd.es/es/documento/ps-00475-2021.pdf

documento de março de 2022 intitulado “Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them”[56] previu uma série de específicos comportamentos que não são compatíveis com a legislação europeia de dados pessoais. São eles: “overloading”, “skipping”, “stirring”, hindering”, “fikle” e “left in the dark”. Acorde o EDPB, são padrões utilizados que, em última análise, servem de técnicas para coleta e tratamento de dados de maneira mais fácil e com menos chances de recusa, discordância ou não consentimento.

Nesse sentido, “Overloading” (ou “sobrecarga”) é ato de impor ao usuário uma avalanche de solicitações, informações, opções ou possibilidades, para que eles compartilhem mais dados ou que permitam o processamento de seus dados involuntariamente ou contra suas expectativas. São exemplos dessa conduta a requisição contínua de fornecimento de dados, com renovação de argumentos para serem fornecidos, vencendo o titular pelo “cansaço”, pois não desejarão mais interromper a navegação com esses pedidos; imposição de dificuldades para obter informações acerca do uso de seus dados e do exercício de seus direitos; e a disposição de muitas e distintas opções de tratamento sem clareza ou didaticidade suficiente. *Skipping* (ato de “pular” ou “ignorar”), por sua vez, significa a projeção de uma interface que induza o titular dos dados a não pensar ou a negligenciar sobre alguns aspectos da proteção de dados. São exemplos a oferta de um “conforto enganoso”, com disposição de opções de coleta e tratamento já previamente selecionados, tornando mais improvável que titulares de dados revoguem tal “escolha” ainda que tenham a possibilidade; bem como a estruturação das informações ou requisições de dados pessoais conjuntamente a outras informações/requisições, provocando possível distração quanto à correta análise das circunstâncias relacionadas aos dados. O *stirring* (“em movimento”) exprime o uso de artifícios visuais ou emotivos para facilitação da coleta de dados. Nesse passo, o uso de palavras, imagens ou sons que incitem o usuário à segurança ou ao medo quando da conferência de consentimento/aquiescência viola os seus direitos enquanto afeta a sua liberdade e informação, ou o uso de recurso visual que leve os titulares à escolha de opções mais invasivas aos seus dados (em exemplo a fixação da opção de aceitação em caracteres grandes e coloridos, e a negativa em caracteres menores e em coloração mais discreta).

Em continuidade ao exame dos padrões indevidos de coleta e tratamento de dados, a prática do *hindering* (ato de “dificultar”) evidencia o procedimento de tornar mais difícil a

[56] Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

informação e gerenciamento de dados pelos usuários. São exemplificações desse comportamento a disponibilização de links de redirecionamento não funcionais; e a exigência do percurso de maior número de etapas para negativa da coleta de dados ou da permissão da coleta apenas para determinadas finalidades do que em comparação com a simples aceitação (com menos etapas).

O procedimento denominado *fickle* ("inconstante") significa o design de interface não claro o suficiente, tornando mais trabalhoso ao titular de dados entender as ferramentas de proteção de dados a ele disponíveis e o entendimento acerca da finalidade do tratamento de seus dados pessoais. Em exemplo se aponta o ato de apresentação das informações sobre dados diversas vezes e em diversos formatos, sem explicação acerca de previsões gerais e específicas e sem ordenamento sequencial didático de informações, tornando confuso o esclarecimento, ou a oferta das explicações sobre coleta e tratamento de dados em aba ou link descontextualizado do tema, de forma a obstar o fácil acesso. Por último, a diretriz da EDPB enuncia o padrão obscuro apontado como *left in the dark*, que em resumo diz respeito à conduta de não conferir a segurança necessária ao titular de dados sobre as informações e finalidades do tratamento de seus dados, de certa forma escondendo tais explicações. Em hipótese, o comitê menciona a disposição de informações em língua distinta da dos usuários do país; e pouca clareza quanto às informações sobre o tratamento dos dados, o que pode induzir à escolha por uma "configuração padrão".

3 OS DESAFIOS DA REGULAÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

3.1 Regulação do tratamento de dados no Brasil e a experiência europeia. Instrumentos e possibilidades

Salomão Filho (2021), em estudo sobre os princípios e fundamentos da regulação da atividade econômica, aponta que por muito tempo se acreditou em uma atuação do Estado como um simples "Estado-polícia", com funções primordiais limitadas à proteção da liberdade econômica e política do particular, ou seja, de mínima atuação e intervenção em atividades. Em oposição a essa atuação "exageradamente liberal" (SALOMÃO FILHO, 2021, p. 110), surgiram os modelos de atuação concernentes à era keynesiana (expressiva intervenção do estado em economias capitalistas) e aos movimentos comunistas revolucionários, com Estados detendo a pretensão de se serem os "grandes gestores do sistema econômico" (SALOMÃO; FILHO, 2021, p. 110). Ambos os movimentos são, nos dizeres do autor, de vertente macroeconômica, em uma ideia de Estado como um gestor máximo, distante e superior do sistema econômico. Em contexto atual, a par das dificuldades de exame do próprio momento histórico em que se vive (a se dificultar o distanciamento do exame), afirma que uma atuação excessivamente distante, a despeito das duas vertentes, não permite ao ente público o cumprimento a contento de suas funções. Há de se admitir a ele,0 Estado, uma função que nem o particular e nem o mercado, por si sós, assumirão, que é a de redistribuir. Essa, segundo Salomão Filho (2021), seria a grande função do "novo Estado", que baseia sua "gestão em valores, e não em objetivos puramente econômicos" (SALOMÃO FILHO, 2021, p. 110). Como abordado de início, a proteção de dados decorre do princípio da privacidade que, por sua vez, deriva da necessidade de proteção do indivíduo, e é ele afinal o destinatário da LGPD. Assim, se o Estado, além da atenção aos interesses pessoais dos cidadãos e mercadológicos, direciona-se de igual modo à gestão de valores, deve voltar também o seu foco à melhor e mais eficiente aplicação da LGPD, pois a sociedade brasileira elegeu, mediante lei, a proteção do indivíduo exposto pelos seus dados como um valor a ser perseguido. Nesse passo, havendo a permanência de problemas relacionados à proteção de dados do cidadão, ao menos sob determinada área de exame (com recorrente busca pelo Judiciário para resolução), e mesmo com a vigência da LGPD, faz-se não apenas útil, mas sobretudo necessária uma maior atuação regulatória do Estado nessa área. A propósito, são os dados pessoais, ao mesmo tempo, um ativo relevante ao agente econômico (dadas as características da sociedade atual) e uma verdadeira projeção da personalidade do indivíduo, que invariavelmente necessita da transmissão de seus dados para

uma vida em sociedade.

Em comparativo abordado no trabalho, demonstrou-se que a singela vigência da LGPD não serviu, acorde dados de pesquisa na jurisprudência do TJSP (capítulo 2; pesquisa realizada entre agosto e novembro de 2023), para refrear de maneira significativa uma pueril forma de violação de dados pessoais: a realização de ligações telefônicas indevidas para clientes ou potenciais clientes de empresas de telefonia sem o prévio consentimento do indivíduo para esse fim específico.

Vale dizer, se as pessoas reclamam perante a Justiça de ligações indevidas efetuadas por empresas que prestam serviços de comunicação, é porque obviamente não concordaram (ou ao menos foram induzidas à concordância sem clareza) que seus dados fossem usados para que lhe endereçassem ligações com distintas propostas. No mesmo sentido, a Lei de proteção de dados não gerou atuação de relevo a impedir que empresas com atividade financeira mirassem alvos específicos para oferta de crédito, valendo-se de informações extraídas de dados sem qualquer clareza acerca da forma pela qual obtidos, o que gerou (e gera) litigiosidade ante os tribunais, pois tal conduta dos agentes não raro gera contratos questionados. Pouco provável assim que instituições com objetivos empresariais passem a obedecer aos ditames da LGPD sem possibilidades de sanção ou recompensa relevantes e decorrentes de eficiente regulação. Inverossímil tal hipótese de "boa vontade" dos agentes econômicos porque os dados pessoais são ativos que permitem aos seus detentores o conhecimento econômico suficiente para elaboração de melhores estratégias visando o lucro. Igualmente dificultoso, em outro vértice, que os indivíduos pura e simplesmente parem de ser potenciais vítimas de tratamento indevido de seus dados, pois, diante das características da sociedade, é inevitável que eles continuem a transmitir dados, uma vez que, como estabelecido anteriormente, para praticamente tudo eles são necessários caso opte ele por viver em comunidade e realizar contratos. Inafastável, portanto, a necessidade de atuação mais efetiva de um Estado gestor na área de proteção de dados, mediante a criação de um ambiente no qual as relações entre os agentes econômicos consigo mesmos, e entre os agentes e o indivíduo, adquiram patamar de maior respeito à LGPD. O referido ambiente a ser criado deve abranger melhoria em todas as relações a envolverem dados:

> Uma regulação com ênfase na criação coercitiva de um ambiente concorrencial incentiva o equilíbrio das forças de mercado, permitindo a difusão do conhecimento econômico. Porém, apenas isso não é suficiente. Sobretudo em setores monopolizados ou oligopolizados, é necessário introduzir regras que operem o reequilíbrio de forma impositiva. Aqui, o reequilíbrio não é mais entre concorrentes, pois não é possível garantir a

> existência de real ambiente concorrencial. O reequilíbrio deve ser entre consumidor e produtor. As medidas devem, portanto, ser diretamente redistributivas (FILHO, 2021, p. 109).

Em um comparativo específico, considerando principalmente o estabelecido anteriormente no sentido de que a legislação e princípios europeus sobre proteção de dados inspiraram nosso percurso até a LGPD, depreende-se que a União Europeia possui, quando em contejo com a realidade brasileira, ambiente regulatório muito mais transparente e detalhado no que toca à atuação dos agentes econômicos. A European Data Protection Board (EDPB – Comitê Europeu para Proteção de Dados), com funções delimitadas no art. 70 da GDPR, dentre elas garantir a consistência e coerência da aplicação da lei de proteção de dados europeia, principalmente na área econômica[57], conforme pesquisa realizada em setembro de 2023[58], apresentava em seu site 71 (setenta e uma) "guidelines" e 8 (oito) "recommendations" sobre os mais diversos temas. O próprio EDPB em seu site adianta que "we issue general guidance (including guidelines, recommendations and best practice) to clarify the law and to promote common understanding of EU data protection laws"[59], reforçando ainda a ideia de fixação e difusão das boas práticas em matéria de proteçao de dados pessoais. Há, nesse contexto, "guidelines" (ou doravante "diretrizes") para regulação do uso de reconhecimento facial; da identificação da autoridade supervisora de um processar de dados; correta informação sobre os direitos subjetivos relacionados aos dados; identificação de padrões enganosos em mídias sociais, e fornecimento de meios para evitá-los; diretrizes para interpretação de artigos específicos da GDPR, obtenção de certificações, realização de transferência internacional de dados, entre outros (EDPB, 2023). Somente em relação ao tópico consentimento, há diretriz específica e praticamente doutrinária sobre a sua regularidade, além de instruções sobre boas práticas com enumeração de exemplos[60], com 33 (trinta e três) páginas apenas sobre essa temática.

Em outro vértice, consoante análise das publicações da Autoridade Nacional de Proteção de Dados (ANPD), autarquia reguladora prevista nos artigos 55-C e seguintes da

---

[57] Disponível em (consulta em 18/09/2023): https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en.

[58] Disponível em (consulta em 18/09/2023): https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en.

[59] Disponível em (consulta em 18/09/2023): https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en. Tradução: "emitimos orientações gerais (incluindo diretrizes, recomendações e práticas recomendadas) para esclarecer a lei e promover o entendimento comum das leis de proteção de dados da UE".

[60] Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

LGPD, depreende-se de seu site que todas as publicações e documentos se encontram em uma mesma aba de pesquisa[61], que contém, em síntese, além dos documentos intitulados "publicações", portarias, resoluções, notas técnicas e relatórios de análise de impacto. Embora se respeite o esforço das autoridades vinculadas ao órgão e o quanto produzido até aqui (pesquisa realizada em setembro de 2023), a extensão e detalhamento dos materiais são deveras distanciados da realidade europeia e das significativas necessidades brasileiras. As publicações não são de número extenso, perfazendo o importe de 14 (quatorze) documentos, dos quais a maioria se refere mais aos conceitos e introdução ao assunto proteção de dados na práxis brasileira. Cartilhas de segurança sobre vazamento de dados e proteção de dados na internet, trato de dados pelo poder público e orientações sobre o uso de cookies são alguns dos temas. As portarias e resoluções mais se vinculam às questões funcionais do órgão, e notas técnicas sobre temas específicos (oito na data da pesquisa). Contudo, pouco sobre interpretação de artigos, práticas nocivas de empresas a serem evitadas, ditretrizes sobre obtenção do consentimento, validade do consentimento, extensão válida do uso de dados pelas empresas, entre outros, temas esses que não são encontrados com facilidade. Pouco também (ou nada no site) há sobre decisões tomadas, multas empreendidas ou publicidade sobre algum ato nocivo detectado.

Por mais não se negue que alguma atuação há, é difícil pontuar que ela é minimamente suficiente, pois sequer as hipóteses simples de realização de ligações inoportunas a clientes ou ofertas sem anterior aquiescência são noticiadas como detectadas, muito embora o tema esteja presente nos tribunais com frequência de relevo, e parte deles já tenha sido objeto de avaliação pela Secretaria Nacional do Consumidor (SENACON).

Pouco se noticia também no site brasileiro medidas tomadas em favor de cidadãos com reclamações individualizadas, o que é recorrente na prática europeia, como se abordou no capítulo segundo, com multas empreendidas e processos nas agências de dados levados a efeito por pleitos particularizados, a indicar uma regulação "pulverizada" e acessível ao indivíduo.

No caso brasileiro, além do fato de se encontrar mais facilmente precedentes de multa administrativa por violação a direitos do consumidor (embora os fatos narrados no trabalho envolvam violação de dados), há indicativo pelas notas técnicas estudadas (e que conforme estudado deram ensejo a multas a bancos, conforme capítulo 2; SENACON, 2019) que a iniciativa de reclamação se deu por parte de instituições especializadas em direito do consumidor, e não por um cidadão isolado. Ou seja, se regulação existe para a proteção de

[61] Disponível em (consulta em 18/09/2023): https://www.gov.br/anpd/pt-br/documentos-e-publicacoes.

dados, ela até aqui se mostra mais eficiente quando a temática é direito do consumidor (a atingir o tema "dados pessoais" reflexamente) e quando o reclamo é capitaneado por uma instituição com maior representatividade, e não por um cidadão, demonstrando a pouca aproximação dos órgãos reguladores perante os titulares de direito, ao menos segundo as reclamações noticiadas neste estudo e que geraram multas administrativas a bancos por violação de dados. Em semelhante sentido, possível se afirmar que esses titulares de direitos pouco sabem sobre seus direitos, afinal pouco diz o Estado sobre o que representa violação de dados pelas empresas, o que por certo prejudica mais a atenção sobre práticas indevidas.

É razoável pontuar, em prosseguimento, que um maior detalhamento permitiria a diminuição da litigiosidade sobre alguns temas que derivam de uso ilícito de dados. E se não é, por certo, indene de dúvidas que uma regulação mais esmiuçada sobre o tema extinguiria os problemas mencionados no capítulo 2, por certo é coerente apontar que o auxílio adviria pelo menos na diminuição da litigiosidade, pois as multas empreendidas não detiveram efeitos nulos (acorde a presente pesquisa). A falta de informação segura prejudica ainda mais o cidadão, que melhor informado de seus direitos e da forma de fazer valer esses direiros, poderia ter seus problemas solucionados antes que maiores problemas ocorressem e antes de precisar acessar o Judiciário. E, se o amparo à resolução de problemas poderia aumentar sob determinado recorte (avaliado segundo o que em parcela se chega ao Judiciário), não se exclui que divulgação das boas práticas seria benéfica semelhantemente ao ambiente regulatório de proteção de dados na totalidade, afinal o conhecimento sobre as condutas e estratégias válidas ou não sob a luz da proteção de dados pessoais seria expandida, o que em tese poderia auxiliar no alcance de um dos objetivos específicos deste trabalho, que é identificar os meios pelos quais seria possível intensificar a eficiência da LGPD na diminuição dos conflitos.

Em reforço dos argumentos, sintomática da atuação distante da ANPD é, segundo os dados avaliados, a primeira multa da mencionada autarquia vinculada à proteção de dados ocorreu em 06/07/2023[62], anos após a vigência da LGPD. Ainda, referida multa, acorde publicação em diário oficial[63], foi direcionada a uma microempresa que se valeu de informações obtidas por aplicativo de conversas para envio de materiais de campanha eleitoral. Vale dizer, grandes empresas de comunicação ou financeiras, que acessam dados com grande frequência e que ocupam polos de processos judiciais também com periodicidade relevante, ainda não ocupam local de importância nas publicações, e menos ainda em notícias de eventual

[62] Disponível em (consulta em 18/10/2023): https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd.
[63] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/2022-62-dou-imprensa-nacional.pdf.

advertência ou multa.

Ainda na esteira de Salomão Filho (2021), a eventual, mais detalhada e presente regulação não se trataria de perene função de "polícia" pelo Estado, mas de instrumento apto ao incremento da cooperação entre os agentes econômicos. A compreensão acerca dos comportamentos devidos aos envolvidos em determinada área contribui com o comportamento do gestor de dados, pois ciente de que aquela diretriz a todos vale. Aliás, o pouco volume de decisões administrativas relacionadas a dados (em específico no que toca às sanções) é demonstrativo de pouca clareza, afinal não se sabe adequadamente do que reclamar, seja o consumidor diante de uma instituição que detenha seus dados, seja um agente em detrimento de seu concorrente. Afora a notícia esparsa da primeira multa aplicada pela ANPS, e a existência de canal específico para denúncias, não é simples a identificação de outras multas aplicadas pelo site (consulta em setembro de 2023). Em comparação, no site da EDPS, em link específico denominado *Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism*[64], depreende-se a notícia de 97 (noventa e sete) decisões de cunho administrativo a envolver distintos países da União Europeia, envolvendo distintos temas, mas todos relacionados à proteção de dados. Relevante ressaltar ainda que a pesquisa não se aprofundou no exame de números de *guidelines* e decisões administrativas existentes nas agências de dados de outros países, a permitir compreensão de que o debate e a influência das agências de proteção de dados é ainda maior. É coerente supor, desta feita, que a regulação mais presente e detalhada, com maior aproximação do que ocorre em solo europeu, contribui para o debate e imposição de condutas que, em última análise, protegem o cidadão, conforme abordado no capítulo 2.

Ainda no que toca à criação de um ambiente que estimule a proteção de dados, e com maior ênfase na relação entre concorrentes, há indicativo de que a maior presença e precisão da regulação pode melhorar a relação entre os gestores das informações dos indivíduos. Conforme aduzido no Capítulo I, em um contexto de "economia da informação" a assimetria de informação por parte de um agente econômico, vale dizer, o fato de uma empresa/instituição financeira deter mais informações derivadas de dados pessoais do que outra, gera problemáticas já avaliadas por estudos de cunho econômico. Por óbvio, quem sabe mais sobre as pessoas pode eleger alvos de mercado que lhe rendam mais frutos. E a violação da LGPD, especialmente quando se debate a invalidade do consentimento, das ofertas emanadas, e a

[64] Disponível em (consulta realizada em 18/09/2023): https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en.

obscuridade do tratamento efetuado, é apta a gerar assimetria em relação às empresas que não praticam as mesmas ilicitudes, prejudicando o ambiente entre os agentes. Assim, valendo-se de uma analogia acerca do "risco moral" gerado pela assimetria de informações, torna-se válido mencionar que o "agente" (a exemplo de um funcionário ou executivo), se dotado de melhores informações, tenderá a tentar a manutenção desse estado e busca dos interesses em prejuízo do "principal" (com menos informações, a exemplo de um patrão ou acionista), perpetuando as "boas decisões" do agente e as "não tão boas" do principal, que desconhece o que se passa.

Na figura do "principal" se pode elencar o concorrente menos informado, que pode se valer da força de uma regulação mais aproximada à europeia a fim de que o conhecimento se dissemine de forma mais clara, ciente de que o regulado é válido para todos e que seu agente melhor informado terá de se adequar às regras, com menor panorama de injustiça. Pode-se elencar na mesma analogia do "principal" a figura do ente regulador, qual seja a ANPD, que pode criar estímulos para que os "agentes" (empresas) obedeçam à LGPD por ocasião de uma regulação mais transparente, detalhada e efetiva, ao prever, delimitar, explicar comportamentos e mesmo os incentivar, a exemplo de conferência de certificados de qualidade e imposição de sanção em caso de desconformidade com as boas práticas. A regulação, enfim, especialmente se tão clara e esmiuçada quanto à europeia, pode gerar estímulos para um ambiente mais sadio sob a ótica da LGPD, e mais especificamente diminuir problemas que não são adequadamente solucionados e deságuam no Poder Judiciário, sob a figura principalmente de ofertas indevidas e contratos indesejados (pois obtidos com violação de dados). E não há explicação do porquê temas como padrões enganosos, diretrizes para o consentimento e interpretação dos artigos da LGPD são tão presentes na Europa e tão ausentes no Brasil, afinal, em uma sociedade da tecnológica e da informação, as grandes empresas que lá atuam aqui também o fazem. O meio pelo qual atuam também é semelhante: mormente o virtual, pela internet.

Dificultoso assim supor que a realidade seja tão díspar a ponto de nosso modelo regulatório ser tão mais tímido. Vale dizer, no sentido do alcance do objetivo específico de se estabelecer comparativos com a experiência regulatória europeia para identificação de paradigmas passíveis de adoção no Brasil, acorde o estalecido, é razoável (senão necessário) que para melhoria do presente ambiente regulatório - que, por enquanto, no tocante à proteção de dados, gera litigiosidade principalmente quando em embate cidadãos e empresas de telefonia e de serviços financeiros - sejam estabelecidas conexões mais próximas à experiência europeia, muito mais acessível e clara do que a nossa, mormente se analisadas as publicações

da European Data Protection Board (EDPB).

Em tarefa de maior ilustração sobre as problemáticas do modelo presente, Cruz (2016), em estudo sobre a assimetria informacional no contexto das finanças corporativas, aponta que a "assimetria é uma anomalia que distorce a eficiência de mercado, gerando efeitos indesejáveis sobre as escolhas dos agentes que dele participam" (CRUZ, 2016, p. 09/10). Nesse passo, disserta que ambientes informacionais mais transparentes e de maior qualidade permitem decisões mais eficientes, aproveitando-se melhor as oportunidades. Como algumas das ferramentas aptas a diminuir a anomalia, aponta a confecção de relatórios financeiros periódicos e a existência de normas e leis para controle de assimetria. Vale dizer, um ambiente regulado (norma em sentido ampla) e avaliado (estudos disponibilizados por órgãos reguladores com enunciação de diretrizes) é apto a incrementar o respeito à LGPD por empresas, valendo-se do raciocínio de que essa obediência em si é saudável ao ambiente, pois coerente com a eficiência do mercado e com a igualdade entre todos os concorrentes. Herscovici (2017), em estudo sobre as certificações e assimetria da informação, aponta que mecanismos de coerção a comportamentos indesejados e gerados por assimetria da informação devem ser capitaneados por terceiros desinteressados, a exemplo das agências regulatórias (em nossa realidade, a ANPD), mais aptos a lidar com distintos interesses. Benacchio e Maciel (2020), por sua vez, ao abordar a LGPD sob a perspectiva da regulação do poder econômico, sustentam que o diploma protetivo de dados é verdadeiro instrumento de garantia da liberdade, privacidade e desenvolvimento dos terceiros seres humanos, principalmente se considerado que as tecnologias de informação atual possibilitam um monitoramento tão relevante de comportamentos humanos, tornando a informação um ativo empresarial. Nesse mesmo sentido, apontam que o domínio da coleta de informações, com maior exclusão de intermediários, integra os modelos de negócio, e que a concentração de dados coletados em um pequeno número de atores (sem "mandato") pode gerar "erosão" da possibilidade de atuação do Estado e de seus instrumentos democráticos.

Em vias de encerramento ao tópico, para além da litigiosidade gerada em razão do uso indevido de dados, por vezes sem consentimento do titular e sem clareza das finalidades da coleta, ofende-se igualmente a liberdade dos cidadãos, principalmente se reconhecido que grandes empresas se valem de coletas massivas de dados, valendo-se Benacchio e Maciel (2020, p. 49) de expressão equivalente a um "colonialismo digital".

Dentre os desafios, apontam a necessidade de mercados mais competitivos, destacando-se alternativas competitivas sempre que possível, bem como o reconhecimento da "natureza sem fronteiras da economia digital, a tornar importante promover maior cooperação

internacional e convergência na aplicação de leis de concorrência" (BENACCHIO; MACIEL, 2020, p. 50). Soluções não apenas "locais" são recomendáveis (embora não se negue a importância da atenção às peculiaridades de cada caso e país), consequentemente, afinal o "mar" digital a praticamente todos é comum, não sendo crível que as recomendações e diretrizes trabalhadas na Europa não sejam fonte relevante de debate e regulação no Brasil, em especial pela ANPD. Uma melhor e mais transparente regulação, assim, pode mais adequadamente "dividir" o poder gerado pela coleta de dados, tornando mais equitativo o ambiente (*ex ante*), municiando, em outro tópico, o cidadão ante as práticas nocivas, considerado o seu melhor conhecimento das práticas e das possibilidades de reclamo. Nesse mesmo desiderato, apontam os mesmos autores a fixação de "prerrogativas" aos titulares de dados, dentre elas o dever de transparência por parte dos gestores, maior controle do destino dos conteúdos e meios eficazes de representação e reparação. Contextos esses que, acorde a pesquisa, ainda são desafios não solucionados pela regulação até aqui levada a efeito, ainda que o acesso a conteúdos de países e grupos de países com semelhante modelo regulatório (como a Europa) seja acessível, mas que podem lograr resolução mais democrática e equânime conforme o proposto neste estudo: hipótese de maior aproximação do modelo regulatório europeu de proteção de dados.

3.2 Paradigmas éticos e autorregulação. Instrumentos

A criação de um ambiente regulatório no qual o conhecimento sobre o que significa proteger efetivamente dados, e seus respectivos benefícios, é coerente com o modelo vivenciado no continente europeu, que possui maior experiência com o tema e com o qual nos espelhamos, e apresenta as suas vantagens, ao menos com a possível diminuição de conflitos. Ainda assim, conquanto um ambiente análogo a esse não seja ainda componente de nosso quotidiano de gestão de dados pessoais, não há de se isentar os agentes econômicos que empreendem tratamento de dados da conscientização e respeito pelos dados das pessoas que com eles dividem o convívio em sociedade, e devem assim tomar parte na iniciativa de resolução dos problemas. Em outras palavras, a ausência de um modelo regulatório tão detalhado e extenso como o europeu não prescinde do olhar as empresas e empresários, uma vez que o esforço para cumprimento da LGPD passa pelos indivíduos e as atividades que eles empreendem. De Lucca (2009), em estudo sobre ética em âmbito empresarial, parte da constatação de que a empresa é elemento fundamental no mundo atual, a ponto de Comparato (1990 apud DE LUCCA, 2009, p. 312) afirmar que ela é "elemento explicativo e definidor da

sociedade contemporânea". Nesse sentido, não bastasse ela prover à subsistência da maior parte da população economicamente ativa do país, produzir a maioria dos bens e serviços utilizados pelo povo, gerar a maior parcela de arrecadação de receitas fiscais e atrair outros agentes econômicos (investidores, fornecedores de serviços, entre outros), ela também influencia comportamentos.

Valores como eficiência técnica, inovação tecnológica e economicidade de meios alcançam também instituições públicas, associações civis e profissionais liberais, e são por elas propagados. De Lucca (2009, p. 312/313) discorre que a empresa é praticamente uma "célula" da economia, e é em seu âmago que se realizam muitas das escolhas que determinam os rumos do desenvolvimento, e que devido ao seu "poder de iniciativa" se encontra na origem da criação das riquezas. Não sem sentido, afora as exceções (como os funcionários públicos), as empresas são locais onde as pessoas passam a maioria de seu tempo, ali produzindo, criando e desenvolvendo. Dado esse panorama, De Lucca (2009), ao abordar a ética tanto como um ideal quanto como uma norma de conduta conducente ao bem, conclui pela relevância de se investigar a forma pela qual a ética age e informa a atividade das empresas.

Desde Warren e Brandeis (1890), ao menos no que tange ao direito de privacidade (aqui entendido como gênese dos estudos sobre proteção de dados pessoais), o indivíduo é reconhecido como o foco maior de atenção da legislação sobre dados pessoais e das autoridades com esse tema relacionadas. A experiência legislativa brasileira, desde a Constituição de 1988, passando pela Lei de Acesso à Informação, Marco Civil da Internet e Lei Geral de Proteção de Dados, reconheceu o valor das informações e progressivamente fixou uma maior proteção aos dados pessoais. Não há de se negar, então, que nossa sociedade adota como um valor de substancial importância a proteção do indivíduo por intermédio da proteção de seus dados, evitando-se daí os possíveis problemas que possam ocorrer. E se empresas, em última análise, são compostas por pessoas que atuam no ambiente brasileiro e que devem, em razão de sua própria humanidade, inserirem-se no mesmo ambiente de convivência harmônica, é coerente que devam espelhar os mesmos valores.

Ao abordar a função social das empresas, De Lucca (2009) reflete que as instituições empresariais devem deter responsabilidade para com o meio em que atuam, mediante um agir consciente e em benefício de todos. Nesse sentido é que se aborda, dentre outros, os deveres das empresas e empresários de não gerar poluição, desigualdades e corrupção, não sendo admitido que a única função de uma empresa seja gerar lucro somente com base em cálculos de custo-benefício e sem respaldo de princípios morais que auxiliem os indivíduos. Mais adiante, o mesmo autor conclui, em busca de uma justificativa filosófica para uma ética

empresarial, que a atividade empresarial em si nada mais significa também que uma profissão voltada à circulação de bens e serviços. E, sendo uma profissão, deve deter tal qual todas as outras um conjunto de normas éticas a serem seguidas, assim como existem as pertinentes a juízes, médicos, engenheiros e outros, no que se denomina usualmente de "deontologia" (a ética específica para determinadas atividades). Mais adiante, se a tutela do indivíduo, de seus dados e de suas informações é um valor caro à sociedade em nosso país, a proteção de dados pessoais deve compor a deontologia das empresas e empresários.

Nessa tarefa específica, em recente estudo sobre as limitações aos sistemas de reconhecimento facial no setor privado, Baccarin (2023, p. 138/139) estabeleceu recomendações, com base na LGPD, às empresas no tratamento de dados obtidos mediante referida tecnologia, no intento de fixação de boas práticas. Tais recomendações são perfeitamente aplicáveis na hipótese deste estudo, pois diversas são as formas de obtenção de dados pessoais (ainda mais agressivas se utilizada a inteligência artificial, que não é recorte desse trabalho). Seja por indução do consumidor a informar seus dados sem real conhecimento da finalidade e necessidade desse ato, pela realização de abordagem sem consentimento prévio, pelo uso de cookies ou por meios de mais refinada tecnologia como a de reconhecimento facial, fato é que o tratamento dos dados pessoais sempre deverá obedecer à LGPD. O referido quadro (doravante denominado "quadro 1"), o qual será também usado como ordem de argumentação (denominado pela autora original de "quadro 6 – Boas práticas em proteção de dados biométricos no uso de tecnologias de reconhecimento facial"; BACCARIN, 2023), é assim descrito (adicionada numeração pelo subscritor, mantidas as demais descrições):

Recomendação	**Justificativa legal (LGPD)**
1) Ter uma finalidade específica, explícita e legítima	Adequação ao princípio da finalidade (art. 6º)
2) Verificar se é necessário para cumprir a finalidade ou se existem meios alternativos mais seguros para isso	Adequação ao princípio da necessidade e adequação (art. 6º)
3) Manter registro dos processos de tratamento de dados conduzido	Adequação ao princípio da responsabilização e prestação de contas (art. 6º)
4) Identificar uma base legal específica para	Adequação ao art. 11 e, quando se tratar de

a finalidade desempenhada e cumprir com seus requisitos	dados de crianças e adolescentes, art. 14
5) Identificar as condições de tratamento dos dados biométricos	Adequação ao princípio da transparência (art. 6º)
6) Garantir que o sistema seja tecnicamente eficaz e suficientemente preciso estatisticamente	Adequação ao princípio da segurança (arts. 6º e 46 a 49)
7) Fornecer informações claras e acessíveis sobre o tratamento dos dados pessoais	Adequação ao princípio da transparência (art. 6º)
8) Cumprir com os princípios de proteção de dados	Adequação ao art. 6º
9) Garantir os direitos dos titulares	Adequação aos arts. 18 a 22
10) Conduzir Relatório de Impacto para avaliação de riscos aos direitos e liberdades dos titulares dos dados e implementação de medidas de mitigação	Adequação aos arts. 5º e 38
11) Adotar uma política de Segurança da Informação	Adequação aos arts. 46 a 51
12) Adotar *Privacy by design and by default*	Adequação aos arts. 46 a 51
13) Implementar código de ética e conduta sobre proteção de dados	Adequação à toda LGPD

Em contextualização com o presente estudo, dentre as 13 recomendações sobre as boas práticas no uso de tecnologia de reconhecimento facial, algumas outras diretrizes específicas de boas práticas podem ser adaptadas e inseridas para as hipóteses de coleta e uso de dados para fins empresariais, especialmente quando se trata de prestação de serviços de cunho financeiro (empréstimos, seguros) ou de prestação continuada a exemplo de um serviço de telefonia, e em acordo à experiência de julgados administrativos europeus, coletadas no capítulo segundo. Em primeiro - e possivelmente mais relevante – plano, há de se ressaltar que jamais uma empresa ou empresário deverá enviar ofertas, ou publicidade para um potencial cliente sem que ele tenha expressamente consentido com isso anteriormente, o que se coaduna com as recomendações 7, 8 e 9 da tabela. Tal nos parece ser, acorde as pesquisas, uma das principais “origens” dos litígios apresentados ao Judiciário, afinal, se o cliente não procurou

pelo serviço, é possível que o adquira sem completo conhecimento das características do ajuste, havendo chance de que tome conhecimento de que o serviço/produto não lhe era realmente necessário. E a problemática, claro, não se subscreve à oferta e publicidade em si, que são lícitas, mas ao uso de dados de cidadãos (como e-mails e telefones) para envio de ofertas de produtos e serviços sem que o cidadão tenha consentido com essa prática.

Em outros pontos no tópico de obtenção consentimento válido, há de se anotar que é inválida a sua obtenção genérica. Nesta reflexão, a existência de "banners" contendo informações sobre os usos que serão empreendidos aos dados coletados não representa consentimento válido, a não ser que haja a simples e acessível possibilidade de escolha pela negativa do tratamento informado. Também, uma simples "declaração de consentimento" sem o esclarecimento devido, conquanto possa ser abordada como "formal" consentimento, não o é para fins da LGPD. Mais clara ainda deve ser a hipótese de consentimento para envio de dados a terceiros que não constam da relação entre a empresa e o cliente, do contrário menos transparente ainda será o controle, e mais dificultoso o exercício de direitos. Em seguimento, e concorde a experiência extrajudicial europeia (capítulo II), a finalidade e a necessidade da obtenção de dados é tema que demanda atenção e maior detalhamento (tópicos 1 e 2 da tabela acima). Em abordagem casuística, se o uso dos dados não for estritamente necessário para o cumprimento do contrato, envolvendo contextos outros como convites para eventos, informações sobre outros produtos e serviços não diretamente relacionados com àquele contratado, a descrição da finalidade deverá ser a mais clara o possível, e com descrições separadas e com acolhimento de consentimento para cada qual (sem uso de um mesmo "feixe" com várias finalidades incluídas). Se dados como telefone ou endereço não forem estritamente necessários, a finalidade de sua obtenção deverá ser precedida da concordância mais clara o possível. E, por concordância mais clara o possível, entende-se por meio das decisões que ela não deve ser "direcionada", seja por uso de cores que induzam o titular (a exemplo de "verde" para maior entrega de dados), seja pela oferta de opções "pré-marcadas" e que exigem a "retirada" da concordância (e não a "inclusão" da concordância), porquanto maior a chance de que o usuário nada exclua. Ainda, a exclusão do consentimento deve ser efetuada de modo tão simples como a empreendida para a sua aquisição, e não por meio mais dificultoso ou com mais etapas. Em tempo, assim prevê a "Guidelines 05/2020 on consent under Regulation 2016/679" (EDBP, 2020, p. 23): "*when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that*

consent equally as easily[65].”

O consentimento para obtenção dos dados e para o uso para determinada finalidade não deve ser condicionado à prestação do serviço ou entrega do produto, a menos que seja necessário e nos exatos limites da necessidade. Em exemplificação, a eventual disposição de isenção de tarifa bancária para o caso de transmissão de dados pessoais (para fins de recebimento de posteriores ofertas, em exemplo) pode até se configurar válida se em exame a “formal” liberdade de contratação de um “pacote” de serviços bancários com uma instituição. Todavia, quando em debate acerca da LGPD, não se mostra lícito o procedimento, pois a isenção se mostra verdadeira indução à remessa de dados, ou mesmo condição a um serviço bancário mais acessível, em contrariedade aos princípios da proteção de dados. O mesmo se diga acerca de condicionamento de fornecimento de dados para atualização de plataformas ou aplicativos. Se é necessário, o dado deve ser exigido. Se não é, deve ser oferecido mediante aceitação incondicionada.

Do contrário, se de forma condicionada forem requisitadas mais informações pessoais como estado civil, hábitos, composição familiar, entre outros, para fins de ofertas (como investimentos), as finalidades deverão ser claramente expostas. Em semelhante sentido, a exigência de dados pessoais para o exercício de direitos, como uma reclamação a uma ouvidoria da empresa, não deve ser exigida além do necessário para a utilização da ferramenta. Em tempo, em qualquer procedimento empresarial a exigência de um dado pessoal será substancialmente legítima quando for necessária e incrementar a performance do serviço a ser oferecido, e não o aumento do lucro e futuros contratos do ente empresarial.

Nessa esteira e em estudo sobre o tema compliance de dados no setor de publicidade digital, Domingues, Miranda e Silva (2021), anotam que os mecanismos sofisticados de tecnologia permitem uma publicidade direcionada, principalmente após a pandemia, quando houve uma maximização do comércio digital. Trabalhando também com as publicações e decisões empreendidas pela SENACON, não negam eles que a melhor identificação de interesses dos consumidores enseja serviço personalizado e que atende os anseios de ambos os polos comprador e vendedor. No entanto, há de se atentar à necessidade de consentimento para manuseio de dados e à vedação de implemento de vantagem diante de um consumidor vulnerável a esses práticas, principalmente em razão da ausência de informação acerca dos dados que a empresa possui. Nesse tópico, o uso de “perfilamento”, caso resulte em

[65] “Quando o consentimento é obtido por meios eletrônicos, com apenas um clique no mouse, deslize ou ou pressionamento de tecla, os titulares dos dados devem, na prática, ser capazes de retirar esse consentimento com a mesma facilidade.”

direcionamento a vulneráveis com a consequente conclusão de contratos ou aquiescência com serviços em verdade não desejados e pouco compreendidos, é medida que viola a LGPD, e contribui com a litigiosidade. Nesse trecho, a adoção de uma política de segurança ou de privacidade pela empresa, passível de ser vistoriada por órgão regulador (que poderá cobrar seu implemento), é medida plausível para diminuição do uso "tóxico" de bancos de dados, afora a construção de um código de conduta direcionado a diretores, funcionários e colaboradores.

Em exame a modelos regulatórios, Domingues, Miranda e Silva (2021) também mencionam uma multa fixada pela SENACON, na qual foi fixada a ilicitude do uso de reconhecimento facial para identificação de preferências de consumo (reações a publicidades fixadas segundo o gênero e a idade da pessoa), pois ausente consentimento, não sendo suficiente eventual menção a "você está sendo filmado", afinal conquanto cientes da gravação, eram inconscientes acerca do uso da tecnologia em nítida assimetria (fornecedor sabe que está direcionando o consumidor, enquanto ele não sabe). Vale dizer, o uso de tecnologia, ainda que mantido o anonimato da pessoa, há de ser precedido de autorização, em modelo a ser seguido por empresas. A possibilidade que o conflito surja após contratação mediante relação assimétrica existe, porque pode o consumidor não compreender realmente qual o real teor do serviço ou característica do produto ao ser a ele direcionado de maneira não espontânea, sem garantia de sua autonomia e independência.

Coligado às recomendações 7, 8, 9, 11 e 13, os mesmos autores estatuem algumas diretrizes para implementação de um compliance de dados pessoais nas empresas, e mais especificamente sob a perspectiva da publicidade (que é relevante meio de coleta de dados, ao menos segundo os casos que deságuam na justiça). Na tarefa de organização mínima de uma estrutura de compliance de dados pessoais, indicam ser essencial o envolvimento de equipe de tecnologia da informação, departamento jurídico, relações institucionais e governamentais e especialistas de mercado, claro, tudo a depender da abrangência da atuação da empresa e às suas especificidades. Adiante, anotam que própria "cultura" da empresa deve ser modificada de dentro para fora, com atualização dos códigos de conduta para adequação aos procedimentos e direitos da LGPD (óbvio, sem descurar do Marco Civil da Internete, Código de Defesa do Consumidor, entre outros). Ao final, assentam programações mínimas de atuação para a estrutura de compliance, a incluir: a já mencionada elaboração de código de conduta que inclua a conformidade à LGPD; avaliação contínua de riscos das atividades (quanto à vulneração de dados) e atualização da "cultura" interna da empresa; fixação de autonomia e independência do setor de compliance; monitoramento constante dos procedimentos da

empresa; disposição de canais abertos e seguros para comunicação de infrações e mecanismos de proteção dos informantes; e, por fim, detecção, apuração e imposição de sanção às condutas em contrariedade ao programa de compliance.

Quanto às programações mencionadas, a estipulação de canal seguro aos indivíduos para reclamo de violação à LGPD representa aproximação ao modelo regulatório europeu. Conforme se verificou em pesquisas vinculadas ao segundo capítulo, relevante parte das sanções empreendidas pelas agências de países europeus derivou de reclamos individuais, ao passo que no Brasil, no que tange às sanções da SENACON (órgão que não vinculado diretamente à proteção de dados), as medidas derivaram em essência de reclamação de instituições voltadas defesa de direitos. Vale dizer, o incremento da possibilidade de que uma atuação individual gere sanções ou respostas quaisquer, em influência de comportamento, representa modelo "pulverizado" e não concentrado em instituições com maior poderio econômico, científico e representativo. Aumenta-se, assim, o potencial preventivo, com certos resultados na diminuição de litígios levados à Justiça, pois haveria aumento de chances de composição e/ou mudança de comportamento da empresa.

Se um abuso no tratamento pode levar a litígios, a exemplo dos perenes questionamentos acerca de contratos realizados com empresa que se vale indevidamente de dados, o arrefecimento desse mesmo abuso pode levar à maior pacificação. Ainda, apontam (DOMINGUES, MIRANDA E SILVA, 2021) que a empresa deve buscar o máximo de clareza e simplicidade no procedimento de tratamento, estimulando que cada funcionário compreenda o melhor o momento de seu contato com dados pessoais, e identifique quais situações rotineiras devem ser avaliadas sob a luz da LGPD, em um compliance de prática constante e não meramente *a posteriori*. Nestes termos, o trabalhador em si deve compreender o momento da coleta e utilização dos dados, quais são os dados, como eles se relacionam à atividade da empresa e o que ocorre com esses dados serem por ele coletados (política de privacidade), instante em que códigos de conduta e "cartilhas" de boas práticas trazidos pelas empresas trariam benefício, pois de cunho elucidativo. Em raciocínio casuístico, se ele empreende o contato inicial, não deve requisitar número de passaporte para determinada atividade se ela não é necessária. E se coleta dados outros, como um perfil de compras, gastos, ganhos, entre outros, deve estar, concomitantemente ao tratamento, ciente de que deve agir em conformidade à LGPD e às normas do código de conduta de sua empresa, evitando problemas ao cidadão proprietário do dado.

Enfim, são inúmeras as ferramentas de autorregulação deferidas às empresas no contexto de proteção de dados, sendo dificultoso aos agentes econômicos a alegação de

desconhecimento. Adiante, não é objetivo do estudo a análise aprofundada de todos esses mecanismos, mas sim a construção do raciocínio de que eles, necessariamente, são intrinsecamente ligados à ética do exercício dos agentes econômicos, dentre empresários e empresas, principalmente os envolvidos com telefonia e contratos a envolver serviços financeiros, pois os litígios judiciais que os envolvem não são insignificantes. E, em nosso interpretar, todas as medidas protetivas de dados permitidas aos atores das atividades empresariais guardam uma relação de essência com o conceito de *privacy by design and by default*, que pode ser traduzido por privacidade por design e por padrão, e está previsto no art. 25 da GDPR.

Em síntese, o referido artigo aponta que:

> "o controlador deverá, tanto no momento da determinação dos meios de processamento quanto no momento do próprio processamento implementar medidas técnicas e organizacionais apropriadas (...) a fim de atender às exigências deste regulamento e proteger os direitos dos titulares dos dados. (...) O controlador deverá implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, somente os dados pessoais necessários para cada finalidade específica do processamento sejam processados. (...) Em particular, essas medidas devem garantir que, por padrão, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas físicas sem a intervenção do indivíduo. Um mecanismo de certificação aprovado nos termos do artigo 42 poderá ser usado como elemento para demonstrar a conformidade com os requisitos estabelecidos nos parágrafos 1 e 2 deste artigo." (GDPR, 2018).

O "espírito" da autorregulação por parte de empresas e empresários se encontra no conceito de *privacy by design and by default*, sendo plasmado nos arts. 50 e 51 da Lei Geral de Proteção de Dados. Em síntese, significa que o próprio design das estratégias e métodos de produção/circulação de bens/serviços deve contemplar, em seu âmago, estratégias e métodos protetivos de dados. Em comparativo prático, se uma empresa voltada à indústria visa estruturar maquinário que seja, ao mesmo tempo, eficiente no aspecto produtivo (aptidão a gerar resultados e cumprir sua função) e seguro (prevenção a danos, como explosão, choques elétricos, poluição, entre outros), não há, acorde a compreensão atual sobre proteção de dados, motivo ético para que a proteção de dados não seja, também, avaliada conjuntamente aos trâmites empresariais, sem dissociação (BIONI, 2019).

Assim, se um banco de dados é formado no âmago da atividade empresarial, a metodologia de sua montagem deve englobar estratégias de proteção de dados, dentre as mais aptas a cumprir com esse desiderato. Ilícito e antiético é a montagem de banco de dados para incomodar cidadãos com publicidades não consentidas ou para direcionar produtos e serviços

a pessoas mais vulneráveis à sua aquisição (como idosos ou aposentados), com resultados danosos na litigiosidade conforme abordado em capítulo anterior.

Bioni (2019), em artigo sobre os desafios da conferência de maior concretude à ideia de *privacy by design* (doravante PbD), aponta que após o fenômeno de assimetria de informação, ocasionado pelas possibilidades amplas de coleta de dados por parte das empresas derivadas do avanço da tecnologia, em uma economia movida por dados, o enfoque do PbD, para além do cuidado à autodeterminação informativa, é principalmente a prevenção de danos. E nesse cenário, os agentes econômicos, sendo os maiores detentores de dados, possuem nítida superioridade informacional em relação a outros atores sociais, e devem compor o cerne das atenções relativas à proteção das informações.

Cita o autor (BIONI, 2019), assim, possibilidades de anonimidade de dados (o que é viabilizado pelo mesmo avanço da tecnologia que permite maior coleta), avaliação mais acurada dos reais interesses por parte do controlador dos dados (agente econômico) e implemento de "meta-regulação". Fundamenta que o referido conceito suplanta a ideia de regulação e autorregulação, exigindo-se que o Estado-regulador fiscalize os processos de gerenciamento de riscos e os procedimentos de transparência empreendidos pelos próprios regulados, em ambiente colaborativo. Dentre os elementos de análise por parte do órgão regulador, a serem implementados pelos regulados, encontram-se: análises de risco (possibilidade de multas ou prejuízos em razão de abusos); *accountability* (transparência, prestação de contas); existência de relatórios de impacto; códigos de boas condutas e conferência de selos (certificações de boas práticas concedidas por terceiros, a funcionar praticamente como um incentivo financeiro). Em outras palavras, um ambiente de corregulação e colaboração, que não dispensa (ao revés, exige) a iniciativa das empresas coletoras de dados, em um "diálogo" regulatório.

Em vias finalização do tópico, por mais que ainda não seja tão clara a regulação sobre proteção de dados, em âmbito teórico e ético não há como desvincular o dever de implemento do respeito à LGPD por parte de empresas e empresários. Em tarefa de autorregulação ou de "meta-regulação" colaborativa, a iniciativa do agente é indispensável, não sendo mais tolerável um ambiente no bojo do qual não se admita um método produtivo que polua o meio-ambiente, mas que ao mesmo se admita como válido o abuso de banco de dados ou a postura agressiva para sua coleta, pois tal postura também lesa pessoas. Do contrário, em plano prático, os problemas para as próprias empresas, especialmente as de telefonia e de serviços financeiros, a envolver principalmente a intensa litigiosidade, não cessarão, por mais se defendam os agentes econômicos pela "licitude" do acordo de vontades entre eles e os

cidadãos.

O possível resultado de maior conscientização do agente econômico (mormente nos casos abordados) pode também conduzir a um debate que gere progresso na construção de um ambiente melhor regulado, afinal as *guidelines* e os outros instrumentos gerados pelos órgãos competentes europeus são também resultados de debates, argumentos e esclarecimentos prestados por todos os envolvidos (cidadãos e empresas) nos processos administrativos. Se a empresa disponibiliza canal para reclamo sobre a LGPD, se ela mesmo fundamenta seus atos com atenção à conformidade de proteção de dados, e se, instada por órgão regulador brasileiro para se explicar sobre qualquer fato, tem ela seus pontos a serem trazidos (pois já sobre eles refletido, com produção de códigos de conduta, exposição de políticas de privacidade, entre outros), já colabora ela com a construção de um ambiente que, ao menos minimamente, aproxima-se do modelo mais claro e democrático sugerido como hipótese para melhor eficiência da LGPD e diminuição de litigiosidade: o europeu.

CONSIDERAÇÕES FINAIS

A ideia de que o indivíduo deve ser protegido não é expediente simplesmente teórico, não devendo somente gerar a atenção de doutrinadores e legisladores que fixem esse ideal em obras ou leis. É, sim, tarefa de todos os que convivem no mesmo ambiente, pois coligados de forma indissociável. Com o avanço da tecnologia e o advento de uma sociedade que se vale do uso de dados para praticamente todas as atividades, é inevitável que os cidadãos transmitam dados pessoais em busca de seus diversos interesses, e que as empresas e empresários os coletem em atenção também aos seus interesses, usualmente voltados ao lucro. A problemática reside na forma pela qual esses dados são coletados e para quais fins esses dados são coletados, haja vista que os agentes econômicos detêm grande potencial de aquisição dessas informações graças à tecnologia e internet. Dentre outros, essa questão também foi um dos motivos para gênese da Lei Geral de Proteção de Dados.

Concomitantemente ao advento da LGPD e aos estudos sobre proteção de dados, depreende-se que a litigiosidade perante os tribunais, principalmente quando em embate consumidores e empresas de telefonia e de serviços financeiros, é ainda significativa. Em estudo a tais casos, a envolver em sua maior parte ligações e publicidades destinadas a pessoas que com elas não concordaram; contratantes que não entenderam bem a proposta de contratação de empréstimos, seguros e serviços financeiros correlatos; ou mesmo cidadãos que negam pura e simplesmente terem aceitado um novo contrato após abordagem, denota-se que no âmago de tais conflitos reside em verdade uma violação à LGPD. A propósito, sem o consentimento não é permitida a abordagem publicitária ou o telemarketing. Sem consentimento, igualmente, não é possível a criação de perfis em bancos de dados para viabilização de abordagem mais eficiente a pessoas vulneráveis e mais tendentes a contratações (como aposentados em relação a empréstimos).

Tais violações, caso não existissem, por mais que não seja razoável afirmar com grau de certeza, não dariam ensejo a seguidos processos judiciais. Ou seja, se nos diplomas legislativos aprovados, em especial a LGPD, a proteção de dados é prevista, a casuística, ao menos nesses casos, não indica que ela é eficiente.

Em acordo ao recorte trazido no estudo, quando em debate publicidades indesejadas e contratos questionados após abordagem não espontânea, o remédio procurado e possibilitado pelo Estado ainda é a ação judicial. Instrumento esse indicado desde o século dezenove, conforme os estudos clássicos de Warren e Brandeis (1890). Assim sendo, ainda é de pouca

validade, na prática, a evolução do tratamento doutrinário e legislativo sobre o tema proteção de dados, afinal o meio de se "consertar" problemas derivados de violação de dados ainda é o mesmo, qual seja, o deságue de reclamações às portas da Justiça.

E esse não deveria ser o resultado em conformidade ao percurso brasileiro até o advento da LGPD. Desde a Lei de Acesso à Informação o Estado Brasileiro reconhece os problemas que a assimetria de informação pode gerar, exigindo dos entes públicos máxima transparência e informação aos cidadãos, no fito de realização de melhor administração e melhores e mais fundamentadas decisões. O valor de uma comunicação sem interferências e eficiente, a exemplo das relações que culminam em contratos, é conquista sedimentada pelo Marco Civil da Internet. Após, com atenção ao indivíduo por detrás das informações transmitidas e das comunicações realizadas, foi deferida a tutela de seus dados pessoais. Assim sendo, é coerente com o percurso realizado na práxis legislativa e doutrinária brasileira que as assimetrias (bancos de dados por agentes econômicos) e as amplas possibilidades de acesso às pessoas não gerem problemas que somente sejam resolvidos por via judicial.

A hipótese proposta é a criação de um ambiente regulatório que mais se aproxime do modelo regulatório europeu. Além da circunstância de a GDPR (Lei europeia para proteção de dados) ter inspirado a criação da LGPD, o modelo centralizado e propositor de regras e diretrizes gerais, e não apenas setoriais, aproxima-se do nosso (a LGPD criou uma Agência específica para trato da proteção de dados). Não há porque não serem aqui abordadas, ainda que mediante pontuações acordes a realidade local, as diretrizes estabelecidas, em sugestão, pelo *European Data Protection Board* (EDPB), que centraliza e organiza a aplicação da GDPR em todo o continente europeu, considerando todos os debates ali ocorridos.

Orientações sobre: a forma de coletar consentimento; possibilitar reclamações sobre dados; fornecer informações; ofertar serviços de forma lícita e sem violação de dados; requisição de dados mínimos, entre outros, são formas claras de atuação e que permitem uma maior e mais segura orientação de todos. Em outro vértice, grandes empresas no Brasil fazem, até este momento, pouco caso de violações como realização de ligações com oferta de serviços, uma básica forma de ofensa a direitos que é pura e simplesmente desprezada. De pouca utilidade, nestes moldes, será um aprofundamento sobre os limites da inteligência artificial se nem o proceder mais básico de adequação à LGPD é respeitado, perpetuando-se os conflitos em seara judicial.

No Brasil, por enquanto, inexiste sistemática transparente e segura nos moldes dos propostos pela EDPB. Obviamente, não se afirma que esta seria a única ou primordial fonte para auxílio no incremento da regulação, mas que inexiste motivo idôneo para não

aproximação ou estudo do quanto lá produzido, haja vista que o avanço tecnológico e a sociedade de informação diminuíram a importância de distâncias e fronteiras (ainda mais se considerado o contato facilitado pela internet).

A criação de um ambiente mais claro acerca do que se pode ou não fazer em matéria de coleta e uso de dados pode facilitar a convivência harmônica entre agentes econômicos entre si (concorrentes) e entre eles e os consumidores. Empresas e empresários podem dirigir sua atenção à atuação lícita cientes de que o combate à assimetria é um móvel da regulação, com vistas a não gerar distorções entre os concorrentes, a facilitar também a fiscalização em relação a todos. Consumidores também terão a seu dispor maior conhecimento de seus direitos, com melhor e mais consciente acesso aos canais de reclamação, tal como já ocorre na Europa. Esse ambiente pode auxiliar a prevenir os litígios, afinal de uma aparente "pueril" violação das regras atinentes aos dados pessoais pode se originar problemas sérios, apenas resolvidos perante o Judiciário.

O recorte da litigiosidade quanto às empresas financeiras e de telefonia é demonstrativo da ineficiência até aqui da LGPD e de seu atual modelo regulatório na área abordada. Além disso, é um demonstrativo do potencial de auxílio que a eficiente aplicação da LGPD pode gerar aos cidadãos. Afora os casos pesquisados, são infindáveis, por certo, as possibilidades de mais respeito aos cidadãos no caso de uma regulação mais clara e eficiente. É nítido, em tempo, que o singelo e clássico ajuste de vontades não é mais capaz de garantir a validade e justeza das relações, sendo necessário maior e melhor aporte regulatório.

Enfim, houve percurso legislativo que logrou o reconhecimento de uma Lei geral protetiva de dados, a Lei Geral de Proteção de Dados. No entanto, ela ainda não é suficiente quanto o possível, afinal a litigiosidade em determinadas áreas (como a de telefonia e financeira) é significativa, e não raro derivada de uma violação à LGPD, ou seja, uma violação aos direitos de um titular de dados. O combate a essas ofensas à LGPD por vias judiciais é meio que não acompanhou a evolução do tratamento do tema. E, após comparativos com a experiência europeia, propõe-se que a adoção de um modelo mais aproximado ao europeu, mais claro, mais detalhado e de constante debate, é apto a auxiliar na prevenção de problemas gerados por violações à LGPD, ou mesmo na resolução do problema antes que ele se torne mais grave ou mais extenso e gere necessidade de ida ao Judiciário.

E, dessa tarefa, não podem se isentar as empresas e empresários. A alegação de "liberdade" de contratação não é essencialmente válida enquanto presente situação de abuso de banco de dados ou uso de dados pessoais em desconformidade com o consentimento livre e consciente. O embate ético que surge após a LGPD, ainda que por ora diante de insuficiente

regulação, é entre o lucro a qualquer custo, sujeito a constante litigiosidade e gerador de insatisfação das pessoas, e a realização de objeto social que contemple em seu âmago o respeito às pessoas, mediante o respeito a seus dados.

Outras formas de coleta e uso abusivo dos dados pessoais podem ser objeto de pesquisas futuras, a exemplo de outras formas de perfilamento (montagem de perfis para bancos de dados) que manipulem as pessoas e as induzam a repassar dados e posteriormente realizarem contratos, podem ser empreendidas. Outrossim, técnicas distintas de possível induzimento de pessoas a empreenderem certos atos e contatos possibilitados pelas informações que delas se têm, tomado como exemplo alguns estudos sobre a “economia da atenção”, também, podem ser objeto de análise futura.

REFERÊNCIAS BIBLIOGRÁFICAS

AGRA, Andressa Dellay; BARBOZA, Fabrício Felipe Meleto. **Segurança de Sistemas da Informação.** Porto Alegre: SAGAH EDUCAÇÃO S.A., 2019.

ARAUJO, Louise; DANESE, Paula Monteiro. **Transferência Internacional de Dados Pessoais: estudo comparado entre a GPDR e LGPD**. In: MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (org.). Lei Geral de Proteção de Dados – Ensaios e Controvérsias da Lei 13.709/18. São Paulo: Quartier Latin, 2020.

ASSI, Marcos. **Compliance – Como implementar**. São Paulo: Jurídicos Trevisan, 2018.

BACCARIN, Cínthia. **As boas práticas em proteção de dados Limitações aos Sistemas de Reconhecimento Facial no Setor Privado Biométricos Faciais.** Dissertação (Mestrado em Direito) – Universidade Estadual Paulista "Júlio de Mesquita Filho", Franca/SP, 2023.

BENACCHIO, Marcelo; MACIEL, Renata Mota. A LGPD sob a perspectiva da regulação do Poder Econômico. In: LIMA, Cíntia Rosa Pereira (coord). **Comentários à Lei Geral de Proteção de Dados.** São Paulo: Almedina, 2020.

BIONI, Bruno et al. (coord.) **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo. Abrindo a "Caixa de Ferramentas" da LGPD para dar Vida ao Conceito ainda Elusivo de *Privacy by Design*. In: DE LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota (coord). **Direito & Internet IV – Sistema de Proteção de Dados Pessoais.** São Paulo: Quartier Latin, 2019.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 de fevereiro de 2023.

BRASIL. Lei 12.527 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 07 de fevereiro de 2023.

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. SECRETARIA NACIONAL DO CONSUMIDOR. Nota técnica nº 243/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ. Brasília, DF: Ministério da Justiça, 2019. Disponível em https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/notas-tecnicas/anexos/nota-tecnica-243.pdf (pesquisa em 25/08/2023, às 07:42). Menção no texto (SENACON, 2019a).

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. SECRETARIA NACIONAL DO CONSUMIDOR. Multa aplicada ao BMG em primeiro grau. Brasília, DF: Ministério da Justiça, 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-multa-banco-por-utilizar-dados-sem-consentimento-de-consumidores-idosos (pesquisa em 25/08/2023, às 07:05 horas). Menção no texto (SENACON, 2019b).

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. SECRETARIA NACIONAL DO CONSUMIDOR. Decisão do recurso sobre multa aplicada ao BMG em primeiro grau. Brasília, DF: Ministério da Justiça, 2019. Disponível em: https://static.poder360.com.br/2022/08/Decisao-no-13_ASSESSORIA-SENACON_GAB-SENACON_SENACON-Decisao-no-13_ASSESSORIA-SENACON_GAB-SENACON_SENACON-DOU-Imprensa-Nacional.pdf (pesquisa em 25/08/2023, às 07:35). Menção no texto (SENACON, 2019c).

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. SECRETARIA NACIONAL DO CONSUMIDOR. Nota técnica nº Nº 35/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ. Brasília, DF: Ministério da Justiça, 2019. Disponível em https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/notas-tecnicas/anexos/114977575_Nota_Tecnica_n__35.pdf (pesquisa em 08/09/2023, às 07:40). Menção no texto (SENACON, 2019d).

BRASIL. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. SECRETARIA NACIONAL DO CONSUMIDOR. Multa aplicada ao banco PAN. Brasília, DF: Ministério da Justiça, 2019. Disponível em: https://pesquisa.in.gov.br/imprensa/servlet/INPDFViewer?jornal=515&pagina=94&data=31/05/2021&captchafield=firstAccess (pesquisa em 08/09/2023, às 07:32). Menção no texto (SENACON, 2019e).

CHINELLATO, Silmara Juny de Abreu; MORATO, Antonio Carlos. Direitos básicos de proteção de dados pessoais, o princípio da transparência e a proteção dos direitos intelectuais. In: BIONI, Bruno et al (coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

COELHO, Fábio Ulhoa; LOTUFO, Mirelle Bittencourt. A Lei Geral de Proteção aos Dados Pessoais e as Investigações Internas das Empresas. In: DE LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota (coord). **Direito & Internet IV – Sistema de Proteção de Dados Pessoais.**São Paulo: Quartier Latin, 2019.

CRUZ, Aletheia Ferreira da. Assimetria informacional no contexto das finanças corporativas: determinantes e efeitos no contexto organizacional. **Rev. Econ. Do Centro-Oeste**, Goiânia, v.2, n.1, pp. 26-39, 2016.

DE LUCCA, Newton; DEZEM, Renata Mota Maciel Madeira. A proteção de dados pessoais no Brasil a partir da Lei n. 13.709/2018: avanço ou retrocesso? In: JORGE, André Guilherme Lemos; ADEODATO, João Maurício; DEZEM, Renata Mota Maciel Madeira (org.). **Direito Empresarial – Estruturas e Regulação.** Volume II. São Paulo: Uninove, 2018.

DE LUCCA, Newton; MACIEL, Renata Mota. A lei nº 13.709, de 14 de Agosto de 2018: a Disciplina Normativa que Faltava. In: DE LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota (coord). **Direito & Internet IV – Sistema de Proteção de Dados Pessoais.**São Paulo: Quartier Latin, 2019.

DE LUCCA, Newton. **Da ética geral à ética empresarial**. São Paulo: Quartier Latin, 2009.

DE TEFFÉ, Chiara Spadaccini; DE MORAES, Maria Celina Bodin. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar-Revista de Ciências Jurídicas**, v. 22, n. 1, p. 108-146, 2017.

DOMINGUES, Juliana Oliveira; MIRANDA, Isabella Dorigheto; SILVA, Breno Fraga M.. Compliance de Dados no Setor de Publicidade Digital: Em Busca Das Melhores Práticas. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas Cueva. **Compliance e Política de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2021.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno et al. (coord.) **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021 (a).

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Revista dos Tribunais, 2021 (b).

EUROPEAN UNION. EUROPEAN DATA PROTECTION BOARD. Guidelines on data protection. Bruxelas, Suíça, 2023. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en (última pesquisa em 25/11/2023).

EUROPEAN UNION. EUROPEAN DATA PROTECTION BOARD. Guidelines on consent under Regulation 2016/679. Bruxelas, Suíça, 2020. Disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (última pesquisa em 27/11/2023).

EUROPEAN UNION. General Data Protection Regulation (GDPR). Bruxelas, Suíça, 2018. Disponível em: https://gdpr-info.eu/art-99-gdpr/ (última pesquisa em 25/11/2023).

FILHO, Adalberto Salomão. Regime Jurídico do Banco de Dados – Função Econômica e Reflexos na Monetização. In: DE LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota (coord). **Direito & Internet IV – Sistema de Proteção de Dados Pessoais.** São Paulo: Quartier Latin, 2019.

FRANK, Robert H.; BERNANKE, Ben S. **Princípios de Economia**. São Paulo: AMGH, 2012.

GETSCHRO, Demi. As Origens do Marco Civil da Internet. In: LEITE, George Salomão e LEMOS, Ronaldo (coords)**. Marco Civil da Internet.** São Paulo: Atlas, 2014.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. A Garantia Constitucional à Inviolabilidade da Intimidade e da Vida Privada como Direito os Usuários no Marco Civil da Internet. In: LEITE, George Salomão e LEMOS, Ronaldo (coords). **Marco Civil da Internet.** São Paulo: Atlas, 2014.

GOVERNO FEDERAL. MINISTÉRIO DA JUSTIÇA. Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Processo Administrativo Sancionador nº 00261.000489/2022-62. Diário Oficial da União: 06/07/2023. Disponível em (consulta em 27/11/2023): https://www.gov.br/anpd/pt-br/assuntos/noticias/2022-62-dou-imprensa-nacional.pdf .

GRUMAN, Marcelo. Lei de Acesso à Informação: notas e um breve exemplo. **Revista debates**, v. 6, n. 3, p. 97-97, 2012.

JARDIM, José Maria. A lei de acesso à informação pública. **Tendências da pesquisa brasileira em ciência da informação**, v. 5, n. 1, 2012.

JOTA, São Paulo, 14/09/2023. Disponível em: https://www.jota.info/coberturas-especiais/seguranca-juridica-desenvolvimento/apos-cinco-anos-da-lgpd-o-que-mudou-e-como-o-mercado-participa-14092023. Acesso em: 25/11/2023.

LAUREANO, Marcos Aurelio Pchek; CORDELLI, Rosa Lantmann. **Fundamentos de Software – Desempenho De Sistemas Computacionais**. São Paulo: Saraiva, 2017.

LEITE, George Salomão e LEMOS, Ronaldo (coords). **Marco Civil da Internet.** São Paulo: Atlas, 2014.

LIMA, Cíntia Rosa Pereira de Lima (coord). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709**. São Paulo**:** Almedina 2020.

LIMA, Caio César Carvalho. Garantia da privacidade e dados pessoais à luz do Marco Civil da Internet. In:. LEITE, George Salomão e LEMOS, Ronaldo (coords). **Marco Civil da Internet** São Paulo: Atlas, 2014.

LISBOA, Roberto Senise. Direito da Sociedade da Informação: a contribuição japonesa. In: LISBOA, Roberto Senise (coord.) **O Direito na Sociedade da Informação IV**. São Paulo: Almedina, 2020.

LOURENÇO, Cristina Sílvia Alves; GUEDES, Maurício Sullivan Balhe. A internet e o direito à exclusão definitiva de dados pessoais na experiência brasileira. In: LEITE, George Salomão e LEMOS, Ronaldo (coords). **Marco Civil da Internet.** São Paulo: Atlas, 2014.

MANKIW, N. Gregory. **Introdução à economia.** São Paulo: Cengage, 2020.

MARTINS, Marcelo Guerra. Análise Econômica do Direito na Sociedade da Informação. In: LISBOA, Roberto Senise (coord.). **O Direito na Sociedade da Informação IV.** São Paulo: Almedina, 2020.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. In: BIONI, Bruno (coord.) et al. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

MICHENER, Gregory; CONTRERAS, Evelyn; NISKIER, Irene. Da opacidade à transparência? Avaliando a Lei de Acesso à Informação no Brasil cinco anos depois. **Revista de Administração Pública,** v. 52, p. 610-629, 2018.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (lgpd) – lei 13.709/2018. In: BIONI, Bruno et al. (coord.) **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SAMUELSON, Paul A.; NORDHAUS William D. **Economia**. São Paulo: AMGH, 2012.

SANTOS, Boaventura de Souza. **A Globalização e as Ciências Sociais**. São Paulo: Cortez, 2002.

SARLET, Ingo Wolfgang Sarlet. Fundamentos Constitucionais: o Direito Fundamental à proteção de dados. In: BIONI, Bruno et al. (coord.) **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPG).** 4ª edição. São Paulo: Saraiva, 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadacini. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11o. In: BIONI, Bruno (coord.) et al. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, Vol. IV, No 5, 1890. Disponível em: <http://civilistica.com/the-right-to-privacy Acesso em 10/01/2023.

ZANATTA, Rafael A. F.; SOUZA, Michel R.O. A Tutela Coletiva em Proteção de Dados Pessoais: Tendências e Desafios. In: DE LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira; MACIEL, Renata Mota (coord). **Direito & Internet IV – Sistema de Proteção de Dados Pessoais.**São Paulo: Quartier Latin, 2019.