UNIVERSIDADE DE BRASÍLIA

LUCAS PEDROSA DE LIMA NOGUEIRA CORRÊA ANDRÉ MARQUES

ANÁLISE DA REGULAÇÃO DO USO DA FERRAMENTA DE *COOKIES* NO BRASIL E NA UNIÃO EUROPEIA

Brasília, 2019.

Lucas Pedrosa de Lima Nogueira Corrêa André Marques

Análise da Regulação do Uso da Ferramenta de *Cookies* no Brasil e na União Europeia

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito da Universidade de Brasília (UnB), como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Pf. Dr. Alexandre Kehrig Veronese Aguiar

Brasília, 2019.

Lucas Pedrosa de Lima Nogueira Corrêa André Marques

ANÁLISE DO USO DA FERRAMENTA DE *COOKIES* NO BRASIL E NA UNIÃO EUROPEIA

Monografia apresentada à Faculdade de Direito da Universidade de Brasília (UnB), como requisito parcial à obtenção do título de Bacharel em Direito, **APROVADO** pela seguinte banca examinadora:

_____

Professor Dr. Alexandre Kehrig Veronese Aguiar,
Doutor em Sociologia pela Universidade do Estado do Rio de Janeiro
Mestre em Direito pela Universidade Federal Fluminense
Professor Orientador

_____

Professora Dr. Laura Schertel Mendes,
Doutora em Direito Privado pela Universidade Humboldt de Berlim
Integrante da banca examinadora

_____

Professor Frank Ned Santa Cruz de Oliveira,
Mestre em Ciências da Computação pela Universidade de Brasília
Doutorando em Filosofia do Direito pela Universidade de São Paulo
Integrante da banca examinadora

Brasília, 24 de junho de 2019.

AGRADECIMENTOS

Agradeço este trabalho a Deus e à Nossa Senhora, pois nada seria possível sem Eles. Aos meus pais, Wilton e Ana Paula, que sempre lutaram para me proporcionar o melhor e me ensinaram todos os valores que carrego comigo. Às minhas irmãs, Anna Karla e Anna Caroline, que me inspiram e possuem minha completa admiração.

A todos os meus amigos, importante fonte de apoio, companheirismo e motivação que transforma qualquer dia difícil em fácil. Agradeço, em especial, ao mestre Thiago Morais, cujo auxílio foi fundamental para a concretização deste trabalho.

Agradeço, também, a toda equipe do escritório Sturzenegger e Cavalcante Advogados, por todos os ensinamentos e compreensão. Sem dúvidas não há lugar melhor para se trabalhar.

Um imenso obrigado aos professores Alexandre Veronese, Laura Schertel Mendes e Frank Ned Santa Cruz, pela confiança e por todos os conselhos.

Por fim, agradeço à Universidade de Brasília, um lugar incrível que proporcionou meu desenvolvimento acadêmico e profissional.

Dedico este trabalho ao meu afilhado, João. Que você nunca perca a curiosidade de uma criança, seja amoroso e respeitoso, e tenha uma vida extraordinária.

RESUMO

O presente estudo busca analisar como é realizada regulação da ferramenta de *cookies* no direito comunitário europeu e no direito brasileiro. Na sociedade da informação os dados pessoais se tornaram importantes para o desenvolvimento econômico. Diante desse cenário, os direitos e garantias fundamentais do ser humano são constantemente ameaçados pelo mercado da vigilância que procura captar a maior quantidade de dados possível. As principais ferramentas de coleta e compartilhamento de dados são os *cookies*, que consistem em marcadores digitais inseridos no disco rígido do computador do usuário pelos *sites* visitados. O trabalho também procura analisar criticamente a potencial efetividade da regulação proporcionada pelo Brasil e pela União Europeia. Para isso, serão comparadas as principais legislações desses dois ordenamentos, e analisados os pontos negativos e positivos de cada uma, indicando, ao final, possíveis soluções para uma regulação efetiva.

Palavras chaves: Dados pessoais – Autodeterminação informacional – Consentimento - *Cookies*

Abstract

In the information society, personal data have become important for the development of the economy. Given this scenario, the fundamental rights and guarantees of the human being are constantly threatened by the surveillance market, which seeks to capture as much personal data as possible. The main tools of data collection and sharing are the so-called cookies, which consist of digital markers inserted in the hard disk of the user's computer by the websites visited. The paper also seeks to critically analyze the effectiveness of the regulation provided by Brazil and the European Union. For this, the main legislations of these two ordinances will be compared, analyzing the negative and positive points of each one, indicating, in the end, possible solutions for an effective regulation.

Keywords**:** *Personal data – Informational self-determination – Consent – Cookies*

Sumário

INTRODUÇÃO

Há muitos anos a sociedade vem se adaptando às facilidades advindas das novas tecnologias. Facilidades, é claro, no sentido de aproximar o cidadão aos seus objetivos, sejam eles econômicos, sociais ou pessoais. No mundo globalizado, pautado pelo capitalismo, essa "facilidade" está quase sempre ligada ao consumo.

Para descomplicar esse raciocínio, pensemos na seguinte situação: um indivíduo que, nos anos 1990, quisesse ouvir suas bandas favoritas, gozava de limitadas opções. Ou ele esperava a sua canção favorita passar na rádio e a gravava em uma fita, ou comprava um CD, ou esperava passar o clipe na televisão etc. Independente da opção, não havia uma forma simples de ouvir músicas comparada a hoje em dia.

Essa necessidade de ter uma canção disponível a todo tempo levou o mercado a desenvolver novas tecnologias para aproximar o indivíduo do seu objetivo, que, nessa situação, era o de escutar suas músicas favoritas. Do *Discman* até o *streaming*, levaram-se anos e diferentes processos para que as pessoas pudessem ter o acesso instantâneo a qualquer música de seus interesses.

Isso ocorreu (e ainda ocorre) em todas as áreas de consumo, e não apenas a musical. As constantes inovações tecnológicas modificaram o comportamento da sociedade até criar uma forma de organização social baseada na transmissão de informações de maneira simples e ágil. Assim ensina o autor Bruno Ricardo Bioni[1]:

> Por isso, a informação avoca um papel central e adjetivante da sociedade: *sociedade da informação*. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedades agrícola, industrial e pós-industrial.

Ainda segundo o autor, os principais destaques dessa mudança estrutural são a Internet e o ambiente digital, ferramentas utilizadas pelo mercado para ocasionar relevantes mudanças no funcionamento da economia. À medida em que a internet foi ganhando cada vez mais usuários, as empresas viram uma oportunidade de criar uma nova espécie de negócio onde poderiam otimizar as suas vendas ao mesmo tempo que diminuíam os seus custos.

[1] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018.

Nesse contexto o e-commerce – ou comércio eletrônico – ganhou uma maior importância e diversos empreendimentos investiram grande parte (ou toda) de suas funções na Internet. Assim surgiram as lojas virtuais, ou seja, empresas que negociam produtos por meio digital, sem necessariamente haver uma loja física, como o caso da grande *Amazon.com, INC*[2].

A constante interação com a internet provocou uma mudança nos hábitos dos consumidores. O meio digital evoluiu e permitiu uma criação e compartilhamento de conteúdo de uma forma nunca vista. Qualquer um pode acessar lojas e produtos no próprio celular sem precisar se locomover, e isso aumentou o número de competidores no mercado, sempre buscando novas formas de otimizar as suas vendas.

No ano de 2017, segundo uma pesquisa realizada pela empresa GSMA[3], o número de smartphones havia chegado à marca de 5 bilhões de unidades. Isso quer dizer que, quanto maior o número de pessoas conectadas, mais conteúdo haverá na cadeia de informações gerada pela Internet. Assim, ter o controle dessa cadeia colocaria em vantagem qualquer empresa que quisesse se destacar no mercado.

Com isso, os dados pessoais[4] dos indivíduos (potenciais consumidores de produtos e serviços) tornaram-se fundamentais para o crescimento das empresas, uma vez que, ao ter conhecimento do comportamento de seus consumidores, podem direcionar com mais êxito as suas atividades. Entretanto, o uso abusivo e desregulado dos dados pessoais pode provocar danos à privacidade e vida íntima dos cidadãos.

Compreender todas as características (como gosto, hábitos e interesses) de determinada pessoa é uma estratégia de mercado utilizada há muitos anos. Entretanto, na atual "sociedade da informação", as novas técnicas e instrumentos tecnológicos possibilitaram o acesso e a

[2] Fundada em meados da década de 1990 pelo empresário Jeff Bezos, a *Amazon.com* iniciou suas atividades de vendas de livros pela internet e tornou-se uma das pioneiras do *e-commerce*. Com o tempo, a *Amazon* ampliou os seus produtos e a forma de entrega, conquistando um lugar dentre as empresas mais valiosas do mundo.

[3] Disponível em: https://www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide-hits-5-billion/ (acesso dia 02/05/2019).

[4] Segundo a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais), dados pessoais são quaisquer informações relacionadas a pessoa natural identificada ou identificável. Compreende-se, portanto, que esses dados não se limitam apenas ao nome, endereço, número de cartão e outras informações de fácil acesso, mas engloba também o padrão de consumo, os horários de maior atividade nas redes sociais, localizações diárias e outros tipos de dados mais complicados de se adquirir.

divulgação desses dados de forma muito mais fácil e rápida, de modo a tornar vulnerável a esfera privada do indivíduo[5].

Esse papel fundamental dos dados dos consumidores na nova economia da informação é descrito da seguinte maneira pelo autor Bruno Ricardo Bioni:

> Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.
> E. com a possibilidade de organizar tais dados de maneira mais escalável (e.g. Big Data), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma "economia de vigilância" que tende a posicionar o cidadão como um mero expectador das suas informações[6].

Sendo assim, para facilitar a captação de dados pessoais dos consumidores, seja para utilizá-los em proveito próprio ou para vendê-los a terceiros, o e-commerce criou diversos mecanismos. Dentre eles está a ferramenta mais comum utilizada pela imensa maioria dos sites, independente do conteúdo: o uso de *cookies*.

Cookies são marcadores digitais introduzidos no disco rígido dos computadores dos usuários pelos *sites* visitados. Eles são capazes de armazenar informações que servem para identificar o usuário e podem causar diversos impactos na vida privada do indivíduo como a produção de um perfil comportamental para a otimização de vendas e o monitoramento de suas atividades *online*.

Desse modo, ao mesmo tempo em que a tecnologia se adapta às exigências da sociedade, a sociedade se adapta para regular essas novas tecnologias. Como o uso indiscriminado dos dados pessoais do cidadão podem violar os direitos de personalidade e privacidade, já celebrados na Declaração Universal dos Direitos Humanos de 1948, nota-se a extrema relevância de se obter uma regulação eficaz para o uso desses mecanismos.

Diante desse paradoxo da informação, no qual o conteúdo é infinitamente reproduzível, o Direito se depara com uma situação de extrema complexidade. De um lado existe a necessidade do compartilhamento de conteúdo para o exercício do direito à informação. Do outro há a possibilidade de violação de diversos direitos fundamentais, sem que o indivíduo consiga perceber imediatamente.

---

[5] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014.

[6] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018.

Nesse contexto, o presente trabalho de conclusão de curso pretende analisar a potencial eficácia e qualidade do ordenamento jurídico brasileiro na salvaguarda dos direitos dos consumidores, especificadamente na regulação do uso da ferramenta de cookies pelos sites do e-commerce. Para isso, será realizado um estudo comparado de conceitos jurídicos e da aplicabilidade da regulação da proteção de dados pessoais no Brasil e na Europa. A União Europeia foi escolhida como base comparativa do presente estudo porque foi a pioneira na criação de regras gerais para a proteção de dados e possui as principais legislações sobre o tema. Além disso, a produção da nova Lei Geral de Proteção de Dados Pessoais do Brasil foi diretamente influenciada pelo Regulamento Geral de Proteção de Dados emanado pela União Europeia, justificando a necessidade de compreensão desse ordenamento estrangeiro.

No primeiro capítulo serão apresentados alguns conceitos relevantes para o tema e a problematização acerca do uso de dados pessoais e o direito de personalidade e privacidade, que serão necessários para justificar a necessidade de uma legislação eficaz de regulação do uso de *cookies*.

No capítulo seguinte, será explicado como a regulação funciona no contexto europeu, segundo um estudo aprofundado de sua legislação. Após, será analisado como o ordenamento brasileiro regula indiretamente o uso do mecanismo de *cookies* por meio do Código Civil, Código do Consumidor, Lei Geral de Proteção de Dados e outras legislações relevantes, uma vez que, ao contrário da União Europeia, não há uma legislação direta sobre o assunto.

No último capítulo, apresentar-se-á a comparação dos modelos europeu e brasileiro, na qual se demonstrarão todos os pontos positivos e negativos de cada um. Por fim, será apresentada uma conclusão acerca da eficácia dos modelos de regulação da proteção de dados pessoais, sobretudo na utilização de *cookies* pelas empresas na internet.

CAPÍTULO 1: DADOS PESSOAIS E DIREITOS DA PERSONALIDADE

Conforme adiantado na introdução do presente trabalho, na atual sociedade da informação o principal insumo que movimenta a economia é a captação de dados pessoais dos cidadãos[7]. Nesse contexto, a constante vigilância dos indivíduos gera efeitos significativos no

[7] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006.

ordenamento jurídico, uma vez que o uso abusivo dos dados pessoais pode violar o direito à privacidade dos sujeitos, exigindo uma mudança na estrutura jurídica.

Um dos reflexos dessa mudança é a constante evolução dos direitos da personalidade, que também sofreu alterações diante da sociedade da informação para buscar a tutela da pessoa humana diante das novas tecnologias. Com a informação no centro da economia, o direito à privacidade está constantemente ameaçado. Entretanto, a sua relação com a proteção de dados pessoais não se confunde, pois um não se limita ao outro.

Relevante se faz notar que a complexidade das relações contemporâneas criou uma nova forma de constituição da identidade do indivíduo que não se limita apenas ao âmbito privado. Surge, então, a necessidade de uma proteção de dados pessoais, capaz de resguardar os direitos dos consumidores dos abusos e excessos oriundos do mercado na tentativa de captação dos insumos para o seu crescimento econômico.

Com o objetivo de facilitar esse entendimento, exploraremos, a seguir, a evolução dos direitos da personalidade que justifica a regulação do uso de dados pessoais, principalmente por meio da ferramenta chamada de *cookies*, uma das mais utilizadas para a captação de dados pessoais, conforme será desenvolvido neste capítulo.

1.1 – Os Direitos da Personalidade na Sociedade da Informação

Os direitos da personalidade foram conquistados ao longo da história, mas passaram a ter uma maior relevância no ordenamento jurídico após a Segunda Guerra Mundial. As atrocidades cometidas nesse período ocasionaram mudanças na ordem mundial, que percebeu a necessidade de uma maior proteção da personalidade humana[8]. Nesse contexto, surge a Declaração Universal dos Direitos Humanos e a proliferação da tutela da dignidade humana nas constituições e códigos de diversos países[9].

Nesse sentido, destaca-se a Lei Fundamental da República Federal da Alemanha de 1949, um dos primeiros textos normativos que estabeleceu o livre desenvolvimento da

[8] FARIAS, Cristiano Chaves de; NELSON, Rosenvald. Curso de Direito Civil 1: Parte Geral e LINDB. 15ª edição. Bahia: Editora *Jus* Podivm, 2017, p. 266.
[9] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018.

personalidade humana como direito fundamental[10], e influenciou diversos ordenamentos jurídicos, inclusive a Constituição Federal Brasileira de 1988. Assim está previsto em seu artigo 2º[11]:

> Artigo 1 [Dignidade da pessoa humana – Direitos humanos – Vinculação jurídica dos direitos fundamentais]
> (...)
> (3) Os direitos fundamentais, discriminados a seguir, constituem direitos diretamente aplicáveis e vinculam os poderes legislativo, executivo e judiciário.
> Artigo 2 [Direitos de liberdade]
> (1) Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral.

Assim, desenvolveu-se a ideia do Estado Social, que privilegia a pessoa humana e reestrutura o Direito com o objetivo de promover a sua proteção[12]. Essa tutela do indivíduo não se resume apenas aos direitos patrimoniais, mas abrange, também, os direitos subjetivos, que são inerentes aos seres humanos.

Nessa ideia, os direitos da personalidade, que envolvem as projeções físicas, intelectuais e psíquicas dos seus titulares, são categorias jurídicas fundamentais para o completo desenvolvimento da dignidade humana[13]. O ordenamento jurídico brasileiro reconhece esses direitos da personalidade, os elencando no capítulo II do Código Civil de 2002, do artigo 11 ao 21. Entretanto, por ser essencial para a preservação da dignidade humana, esses direitos não são imutáveis e, ao contrário disso, estão em constante evolução.

Devido à sua "elasticidade",[14] os direitos da personalidade sofreram mudanças essenciais na atual sociedade da informação. Os inúmeros dados produzidos cotidianamente criaram um paradigma para a tutela da dignidade humana, permitindo uma abertura para que a proteção de dados pessoais entrasse como uma nova espécie de direito da personalidade.

Entretanto, pergunta-se a razão pela qual a proteção de dados pessoais não estaria tutelada somente pela ótica do direito à privacidade, uma vez que os dados pertencem à pessoa

---

[10] Ibidem.
[11] ALEMANHA, *Deutscher Bundestag* , 1949, disponível em: https://www.btg-bestellservice.de/pdf/80208000.pdf. Acesso dia 21/05/2019.
[12] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006.
[13] FARIAS, Cristiano Chaves de; NELSON, Rosenvald. Curso de Direito Civil 1: Parte Geral e LINDB. 15ª edição. Bahia: Editora *Jus* Podivm, 2017, p. 267.
[14] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 58: "Daí porque os direitos da personalidade fazem parte de uma cláusula geral de proteção de tutela e promoção da pessoa humana ou de um sistema geral de tutela à pessoa humana, cuja consequência principal e a sua *elasticidade*. Os direitos da personalidade são uma 'noção inacabada' que deve ser cultivada'".

e deveriam afetar a esfera individual de cada um. É verdade que a proteção de dados está diretamente relacionada à vida privada do indivíduo, mas não se limita a isso. Explica-se.

1.1.1 Direito à Privacidade e Proteção de Dados Pessoais

O direito à privacidade, ou direito à vida privada, conforme alguns autores chamam, varia de acordo com tradições e costumes, podendo sofrer limitações conforme os valores de cada povo. No entanto, a privacidade nem sempre foi um assunto relevante para os tribunais. Nos séculos passados, antes da propagação rápida de informação de fatos da vida privada por meios de comunicação de fácil acesso, a tutela da intimidade perdia espaço para a proteção da propriedade.

O primeiro indício da preocupação com o direito à privacidade se deu no final do século XIX, quando dois advogados, Samuel Warren e Louis Brandeis, publicaram o famoso artigo, *The Right to Privacy*, pela *Harvard Law Review*, no qual procuraram princípios e precedentes na *Common Law*, para que se pudesse defender a privacidade dos indivíduos[15]. Eles apontavam como as novas máquinas, jornais e fotografias invadiam a esfera privada dos cidadãos, e que, por isso, havia a necessidade de se criar meios de proteção para garantir o *right to be let alone* (direito de ser deixado só)[16].

Posteriormente, essa proteção tornou-se um direito fundamental e uma das garantias de desenvolvimento da personalidade do ser humano. Mas a forte influência da concepção individualista dos autores pioneiros do direito à privacidade ainda permaneceu em algumas garantias que tutelam a privacidade.

Nesse sentido, pode-se dizer que a vida privada ainda tem um caráter individualista, caracterizada pela proteção das particularidades de cada sujeito sem a interferência da coletividade. Ou seja, o direito de ter a sua vida pessoal e íntima protegida, sem a divulgação de suas particularidades a terceiros, a não ser aquelas permitidas pelo próprio titular[17].

---

[15] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O Direito à Proteção de Dados Pessoais e a Privacidade. Curitiba: Revista da Faculdade de Direito – UFPR, nº53, 2011, p. 53.

[16] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 28.

[17] FARIAS, Cristiano Chaves de; NELSON, Rosenvald. Curso de Direito Civil 1: Parte Geral e LINDB. 15ª edição. Bahia: Editora *Jus* Podivm, 2017, p. 268.

Pode-se notar, por exemplo, a influência dessa individualidade no Brasil, uma vez que a Constituição Federal de 1988 compreende que deve ser protegido do conhecimento de terceiros tudo aquilo que diz respeito à esfera íntima do sujeito[18]. A tutela promovida pela a Carta Magna pode ser observada nos seguintes incisos do seu artigo 5º:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> X - são invioláveis a 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;
> (...)
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> (...)
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Existem, portanto, no ordenamento pátrio, duas dimensões do direito à privacidade: uma ligada à vida pessoal, como orientação sexual, ideologia, religião etc., e outra relacionada à publicização dos fatos derivados da vida do indivíduo. Contudo, apesar da intimidade da pessoa humana ser inviolável[19], o direito a não publicização de determinadas informações pode ser mitigado. Isso ocorrerá quando for necessária a defesa de um bem jurídico mais denso[20].

Diante dos avanços da tecnologia, que possibilitaram o processamento de dados da vida privada de maneira ainda mais rápida, fácil e ilimitada, em comparação com a época em que o *Right to Privacy* foi publicado, o direito à privacidade ficou cada vez mais ameaçado. Surge, então, um embate entre o avanço tecnológico e a salvaguarda da vida privada, no qual um iria sempre tender a limitar o outro. Entretanto, a busca de uma harmonização entre a inovação e a preservação da privacidade dos cidadãos se mostra a melhor maneira de resolver esse conflito[21].

Dessa forma, assim como a própria tutela da personalidade humana precisou de mudanças para se adequar à atual sociedade da informação, o conceito de privacidade também

---

[18] Ibidem.

[19] Assim dispõe o artigo 21 do Código Civil de 2002: "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

[20] FARIAS, Cristiano Chaves de; NELSON, Rosenvald. Curso de Direito Civil 1: Parte Geral e LINDB. 15ª edição. Bahia: Editora *Jus* Podivm, 2017, p. 269.

[21] GARFINKEL, Simon. *Database Nation: the death of privacy in the 21th Century*. California: O'Reilly Media, 2000, p. 5. *apud* MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 34.

passou por um processo de evolução. No decorrer do século XX, a definição originária do *right to be let alone*, passou para uma nova dimensão, onde o indivíduo tem o direito de controlar suas informações e construir sua vida privada do modo que bem entender.

Nesse contexto, Danilo Doneda, em sua tese de doutoramento, relaciona a evolução do conceito de proteção da privacidade ao surgimento da disciplina de proteção de dados pessoais. Afirma:

> A necessidade de funcionalização da proteção da privacidade faz, portanto, com que ela originasse uma disciplina de proteção de dados pessoais, que compreende pressupostos ontológicos idênticos aos da própria proteção da privacidade: pode-se dizer que é a sua "continuação por outros meios"[22].

Destarte, ao seguir com esse "legado" da proteção da privacidade, essa disciplina esbarra em inúmeros novos interesses advindos da sociedade pós-industrial, fazendo com que assuma diversas características próprias e demonstre a necessidade da superação dos antigos conceitos que limitavam o direito à privacidade a uma tutela de natureza patrimonialista[23].

Nesse sentido segue o raciocínio da autora Laura Schertel Mendes, que, em seu livro *Privacidade, Proteção de Dados e Defesa do Consumidor*, conclui:

> Nesse contexto, percebe-se uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros. Dessa forma, opera-se na dogmática e na prática jurídica uma clara evolução no direito à privacidade[24].

Por outro lado, o autor Bruno Ricardo Bioni defende que vincular a proteção de dados pessoais ao direito à privacidade seria um equívoco, pois a construção desse direito possui como base o conceito de dados pessoais, e a sua normatização depende de autonomia para que possa regular o fluxo de informações como um "fator promocional da pessoa humana".[25]

Segundo o autor, a privacidade se relaciona com a liberdade negativa do indivíduo, ou seja, uma "não ação" do Estado ou da coletividade para que não intervenham na sua vida privada. A proteção dessa privacidade estaria inserida na divisão entre o público e privado,

[22] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006, p. 27.
[23] Ibidem.
[24] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 32.
[25] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 100.

sendo um direito estático[26] que só atua quando os fatos definidos pelo próprio titular como privados, forem violados e expostos na seara pública.

Entretanto, o direito à proteção de dados pessoais consiste em uma liberdade positiva, que exige controle das informações pessoais, sejam elas públicas ou privadas. Logo, esse direito funciona fora do binário público-privado, diferenciando-se substancialmente do direito à privacidade[27]. Compreende-se, ainda, que existem diversas liberdades individuais que não são tuteladas pelo direito à privacidade, mas são acolhidas pela proteção de dados.

Isso significa, por exemplo, que mesmo que alguns bancos de dados possuam fatos públicos de um indivíduo (ou seja, foge da sua vida privada), estarão sujeitos à proteção de dados pessoais, uma vez que essas informações atreladas com outras podem causar danos ao seu titular.

Nesse sentido, a evolução do direito à privacidade mudaria qualitativamente[28] a sua concepção em comparação à originária. De um direito negativo e estático, passaria a ser positivo e dinâmico, permitindo ao seu titular o controle de suas informações pessoais e construção da própria vida privada.

Entretanto, esse panorama gera certas incertezas para a dogmática jurídica. Cabe aqui, a ponderação de João Carlos Zanon acerca da percepção da proteção de dados pessoais como uma evolução do direito à privacidade:

> Esse quadro traduz uma reflexão: seria essa forma de redefinição do direito à privacidade a melhor maneira do Direito nacional lidar com o advento das necessidades da contemporânea sociedade da informação? O ponto de partida para responder essa indagação, em nosso sentir, parece estar em considerar que essa evolução do direito à privacidade não significa – e não pode significar – uma superação dos velhos problemas de intromissão indevida na esfera íntima e na vida privada dos indivíduos. Esses antigos conflitos, a que poderíamos denominar de clássicas violações à privacidade, continuam existindo, sendo, aliás, cada vez mais recorrentes[29].

[26] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 96.
[27] BIONI, Bruno Ricardo; RIBEIRO, Márcio Moretto: A transposição da dicotomia entre o público e privado. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-transposicao-da-dicotomia-entre-o-publico-e-o-privado. Acesso dia 24/05/2019.
[28] RODOTÁ, Stefano. A Vida na Sociedade da Vigilância. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 7.
[29] ZANON, João Carlos. Direito à Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2013, p. 63, *apud* BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 98.

Portanto, a limitação da proteção de dados pessoais como uma espécie vinculada ao direito de privacidade não corresponde ao real alcance da sua tutela, o que poderia inviabilizar a sua normatização[30]. A autonomia da proteção de dados pessoais se torna essencial na medida em que o bem jurídico tutelado por ela foge, muitas vezes, da tutela do direito à privacidade. Portanto, o direito à proteção de dados pessoais deve ser alocado como um novo direito fundamental de personalidade.

1.1.2 A Garantia Constitucional da Proteção de Dados Pessoais como Direito Fundamental

Antes de seguir com a exposição acerca da garantia constitucional da proteção de dados pessoais como direito fundamental, faz-se relevante a análise do que seria considerado dado pessoal. Segundo a definição mais recente promovida pela Regulação Geral de Proteção de Dados da União Europeia, dados pessoais consistem em[31]:

> Artigo 4.o Definições
> Para efeitos do presente regulamento, entende-se por:
> 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

O regulamento também possui definição expressa de (i) dados genéricos, que são relativos à características genéticas, hereditárias ou adquiridas de uma pessoa que tragam informações únicas sobre a fisiologia da pessoa ou a sua saúde que resulte de análise de uma amostra biológica do titular; (ii) dados biométricos, que resultam de uma tratamento técnico específico relativo a características físicas e comportamentais que permitam a identificação do indivíduo, como feições faciais; e (iii) dados relativos à saúde, que se relacionam com a saúde física e mental do titular, incluindo prestações de serviços de saúdem que podem identificar o estado do indivíduo[32].

[30] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 100.
[31] EUR-LEX. Regulamento (UE) 2016/679 do Parlamento europeu e Conselho, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso dia 25/05/2019.
[32] MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo, Thomson Reuters, 2018, p. 39.

Apesar de não trazer expressamente a definição de dados sensíveis, o regulamento continua com a definição trazida pela Diretiva 95/46/CE de que dados sensíveis são todos aqueles capazes de revelar a origem racial ou ética do cidadão, as opiniões políticas, religião, filiação partidária ou sindical, dados biométricos, dados relativos à saúde e orientação sexual.

No Brasil, a Lei Geral de Proteção de Dados pessoais, inspirada da RGPD, traz os mesmos princípios conceituais de dados pessoais e dados sensíveis. Assim está disposto na Lei nº 13.709/2018[33]:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: 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, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

As primeiras normas de proteção de dados visavam o controle do uso de informações pessoais pelo Estado. Os primeiros casos que abriram a controvérsia acerca do uso da informática para a captação e armazenamento de dados pessoais dos cidadãos foram o *National Data Center*, nos Estados Unidos, e o projeto *SAFARI*, na França[34]. Já na década de 1970, surgiram as primeiras legislações que tentavam limitar a coleta de dados pessoais (predominantemente pelo próprio Estado) pelo risco aos direitos de personalidade.

Entretanto, o principal caso responsável pela discussão acerca da proteção de dados como direito da personalidade e despertou a preocupação de outros ordenamentos jurídicos sobre essa necessidade, foi a Lei do Censo de 1983, na Alemanha. Essa lei determinou a coleta de todos os cidadãos para fins de estatísticas da distribuição espacial e geográfica da população. Além disso, ela previa que todos os dados coletados poderiam ser compartilhados e cruzados com outros registros públicos e transmitidos para autoridades federais, além de impor uma multa pecuniária para todos que não respondessem as pesquisas[35].

Isso gerou várias indignações por parte da população e, mesmo já havendo uma lei sobre a regulação de dados pessoais, ela se demonstrou incapaz de solucionar o caso, levando a

---

[33] BRASIL. Lei nº 13.709/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso dia: 25/05/2019.

[34] Sobre esses casos, vide: DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006, capítulo 2.2.

[35] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006, p. 193.

matéria para a Corte Constitucional Alemã. A Corte julgou a lei parcialmente inconstitucional, com base nos artigos 1.1 e 2.1, da Lei Fundamental Alemã, que justamente tratam sobre a estrutura geral dos direitos de personalidade, e considerou que o compartilhamento dos dados coletados deveria ter a única finalidade de estatística.

Com essa decisão, a Alemanha trouxe ao menos dois aspectos relevantes para a disciplina da proteção de dados: a consideração desse direito como um direito de personalidade autônomo, com a utilização do termo autodeterminação informacional para além do consentimento, e a função e os limites do consentimento do titular dos dados.[36]

A autodeterminação informativa foi uma extensão das liberdades do indivíduo, estabelecendo a importante noção de que os cidadãos possuem o controle das suas informações, reconhecendo que o tratamento de dados era um processo e não se encerrava no simples consentimento de sua utilização, que foi considerada como uma das fases do processo.[37]

Outro fator importante dessa decisão foi a desconstrução da compreensão de que certos dados eram irrelevantes para a privacidade, uma vez que a Corte Constitucional Alemã, no julgamento da Lei do Microcenso, de 1957, entendeu que apenas os dados pessoais relativos à intimidade dos cidadãos seriam passiveis de proteção[38].

Dessa forma, o caso da Lei do Censo foi decisivo para a construção da proteção dos dados pessoais como um direito autônomo da personalidade, desvinculando-o da divisão público-privado. Portanto, ao interpretá-lo como um direito fundamental baseado nos artigos 1.1 e 2.1, compreende-se que há uma constitucionalização da proteção de dados pessoais no ordenamento jurídico alemão.

Nesse contexto, também é possível verificar a preocupação de outros países em reconhecer o direito de proteção de dados como fundamental[39]. A Constituição de Portugal, por exemplo, regulamenta essa matéria no seu artigo 35º, transcrito abaixo[40]:

Artigo 35.º

[36] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 101.
[37] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Revista Espaço Jurídico. Vol. 12, nº 2. Joaçaba: Unoesc, 2011, p. 91 – 108.
[38] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 104.
[39] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 172.
[40] PORTUGAL, Constituição da República Portuguesa, disponível em: https://www.parlamento.pt/Legislacao/paginas/constituicaorepublicaportuguesa.aspx. Acesso dia 24/05/2019.

> Utilização da informática
> 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
> 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
> 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
> 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.
> 5. É proibida a atribuição de um número nacional único aos cidadãos.
> 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
> 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

Outro exemplo é a Constituição da Espanha, que assegura a limitação do uso da informática para proteger os direitos da personalidade, dispondo da seguinte maneira[41]:

> Artículo 18.
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

A União Europeia, com o objetivo de reforçar os direitos fundamentais aos Estados-Membros, instituiu a Carta dos Direitos Fundamentais da União Europeia, que também reconhece expressamente a proteção dos dados pessoais como um direito fundamental, dispondo da seguinte maneira[42]:

> Artigo 8.o
> Proteção de dados pessoais
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[41] ESPANHA, Constitución Española, disponível em: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf. Acesso dia 24/05/2019.
[42] EUR-LEX. Carta dos Direitos Fundamentais da União Europeia, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso dia 24/05/2019.

No Brasil, a proteção de dados pessoais ainda não é objeto previsto diretamente na Constituição Federal. Conforme depreende-se do subitem anterior, os direitos dispostos no art. 5º, inciso X e XII, da Carta Magna, relativos à inviolabilidade da vida privada e íntima, além do sigilo da correspondência e comunicações, não são suficientes para tutelar, por eles mesmos, o direito à proteção de dados pessoais[43].

Sendo assim, mostra-se necessário uma reinterpretação das garantias constitucionais para enquadrar esse "recente" direito fundamental como complemento do direito ao sigilo e à vida privada e íntima. Um dos elementos principais para essa nova interpretação constitucional é a ação intitulada de *habeas data*, introduzida no art. 5º, inciso LXXII, da Constituição Federal, que determina:

> Art. 5º
> (...)
> LXXII – conceder-se-á habeas data:
> a) Para assegurar o conhecimento de informações relativas à pessoa impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) Para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Esse instrumento reconhece a proteção constitucional das informações pessoais que, ao ser interpretado juntamente ao princípio da dignidade humana, cria espaço para a ampliação dos direitos à proteção da privacidade e intimidade e do sigilo de informação e comunicação, à proteção de dados pessoais[44]. Assim compreende o Superior Tribunal de Justiça, exemplificado pelo voto da Ministra Nancy Andrighi, assim emendado[45]:

> EMBARGOS DE DECLARAÇÃO. RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. BANCOS DE DADOS. PROTEÇÃO AO CRÉDITO. PRIVACIDADE E INTIMIDADE. AUTODETERMINAÇÃO INFORMATIVA. DIREITOS FUNDAMENTAIS. EFICÁCIA HORIZONTAL. PRINCÍPIO DA MÁXIMA EFETIVIDADE. OBRIGAÇÃO DE NÃO FAZER. ANOTAÇÕES. CARTÓRIOS DE PROTESTO. TERMO INICIAL DO PRAZO. ART. 43, § 1º, DO CDC. DATA DO VENCIMENTO DA DÍVIDA. MODULAÇÃO DOS EFEITOS. ART. 927, § 3º, DO CPC/15. PRINCÍPIO. PROTEÇÃO DA CONFIANÇA LEGÍTIMA. REGIME DE TRANSIÇÃO. ART. 23 DA LINDB. ÔNUS E PREJUÍZOS ANORMAIS OU EXCESSIVOS.

[43] Nesse sentido, MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 165: "Vê-se, assim, que, embora as garantias de sigilo e de inviolabilidade da intimidade e da privada configurem importantes mecanismos de proteção individual, eles se mostram insuficientes para lidar com os atuais efeitos do processamento e utilização da informação sobre o indivíduo. Afinal, essas garantias visam à proteção específica em face de riscos determinados (...) e não abarcam a totalidade dos riscos aos quais o indivíduo está submetido na sociedade da informação".

[44] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 172.

[45] EDcl no REsp 1630659/DF, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 27/11/2018, DJe 06/12/2018, grifou-se.

> (...)
> 7. Os direitos à intimidade e à proteção da vida privada, diretamente relacionados à utilização de dados pessoais por bancos de dados de proteção ao crédito, consagram o direito à autodeterminação informativa e encontram guarida constitucional no art. 5º, X, da Carta Magna, que deve ser aplicado nas relações entre particulares por força de sua eficácia horizontal e privilegiado por imposição do princípio da máxima efetividade dos direitos fundamentais.
> (...)

Entretanto, como já foi defendido anteriormente, a interpretação extensiva da privacidade como maior fundador para a égide constitucional da proteção de dados pode limitar sua atuação. Nesse sentido, a Comissão de Constituição, Justiça e Cidadania (CCJ) aprovou, no dia 22/05/2019, a PEC 17/2019[46]. Essa proposta à Emenda Constitucional pretende acrescentar os incisos XII-A, ao artigo 5º, e XXX, ao artigo 22, da Constituição Federal, para incluir a proteção de dados pessoais dentre os direitos fundamentais, algo basilar para o reconhecimento desse direito como autônomo.

1.1.3 Limites do Direito à Proteção de Dados Pessoais

Diante do exposto, verificou-se que a sociedade da informação criou a necessidade de uma reinterpretação do Direito para que a proteção de dados pessoais seja reconhecida como um direito fundamental. Contudo, faz-se necessário compreender que esse direito não é absoluto, e pode ser mitigado em determinadas situações concretas.

A própria Corte Constitucional alemã, em sua decisão no caso da Lei do Censo, previu importantes limitações à autodeterminação informativa, quando contrapor interesses públicos previstos em lei. No Brasil, além disso, para que a limitação seja constitucional, deve haver a aplicação do princípio da proporcionalidade, previsto no artigo 5º, inciso XII, da Constituição Federal. Assim, quanto maior a violação da personalidade do indivíduo, maiores os requisitos para a intervenção e mais específica a legislação deve ser[47].

[46] BRASIL. PEC 17/2019, Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso dia 26/05/2019.

[47] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 188.

1.2 – *Profiling* e *Big Data*: Os Riscos da Coleta e Processamento de Dados

Com o desenvolvimento do mercado no contexto da era digital, os dados pessoais dos consumidores, cuja produção cresce exponencialmente todos os anos, tornaram-se essenciais para o funcionamento e desenvolvimento da economia. A internet permitiu que os consumidores compartilhassem informações sobre produtos e serviços com maior frequência, auxiliando o processo de produção dos objetos de consumo, que são, agora, modelados de acordo com as opiniões diretas dos cidadãos.

Dessa forma, os consumidores não são mais o agente final do ciclo do consumo, e recebem uma posição relevante que condiciona a produção, distribuição e segmentação do bem de consumo[48]. Ademais, por meio de diversas ferramentas, como os *cookies*, o mercado consegue coletar diversos dados do usuário, como localização geográfica, hábitos de consumo e emoções, que podem ser captadas, por exemplo, de acordo com as músicas e pesquisas do usuário em determinado momento.

Isso oferece um rico conteúdo para que as empresas possam direcionar anúncios de produtos e serviços com maior probabilidade de venda para determinado consumidor. A captação *online* dessas informações tomou um rumo nunca imaginado antes e quase impossível de se realizar *offline*. Por meio dessa coleta, torna-se possível constituir um perfil comportamental do consumidor com muita exatidão, devido ao constante monitoramento.

Dessa forma, os dados pessoais possuem grande valor pecuniário para as empresas. Um serviço *online* que se diz gratuito, na verdade, está captando dados relevantes que podem oferecer lucros à empresa com o seu processamento. Enquanto alguns negócios ganham dinheiro com o uso direto das informações proveniente da captação de dados, outras se sustentam com a venda deles.

Muitas vezes o próprio usuário não tem noção de como e para que motivo os seus dados serão utilizados, mesmo consentindo com a sua captação. Há, portanto, uma crítica à autodeterminação informacional, justamente porque o titular não sebe qual será o custo efetivo dessa transação, impondo a necessidade de uma limitação do consentimento[49].

[48] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 15

[49] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 28

Portanto, o acúmulo e processamento dos dados pessoais podem causar danos inimagináveis e de difícil percepção pelos consumidores, tendo em vista o abuso da utilização desses dados que extrapolam o seu fim concedido e violam seu direito fundamental.

1.2.1 *Big Data*

O grande volume de dados virtuais produzidos todos os dias precisa ser estruturado e analisado para que possam ter utilidade. O termo *Big Data* nasceu para denominar essa tecnologia de processamento de dados, estando relacionado à "3 Vs": velocidade, volume e variedade[50]. No *Big Data*, a necessidade de os dados estarem estruturados para o seu tratamento é desnecessária, pois são analisados em toda a sua extensão com o apoio de algoritmos que permitem alcançar diversos fins, dependendo daquilo que a empresa deseja.[51]

Em síntese, essa metodologia permite o processo e organização de dados em diversos formatos para que se possa extrair informações relevantes e, inclusive, prever acontecimentos futuros por meio de análise de probabilidade. Com o cruzamento de dados e a interpretação deles, é possível verificar a relação entre informações e estabelecer padrões. Por esse motivo, os dados são fatores preciosos para otimizar a venda de serviços e produtos, e, até mesmo, verificar o perfil de um indivíduo para, por exemplo, concessões de crédito e contratação em empregos.

Cabe, aqui, diferenciar dados de informação. O primeiro diz respeito a símbolos, sinais, algoritmos e formas armazenados em algum suporte material, que existem independentemente de qualquer interpretação. O segundo consiste em qualquer ação interpretativa que depende de um observador. Os dados são, portanto, potenciais de informação (ao serem interpretados, geram alguma informação).[52]

Um exemplo da ação do *Big Data* é o caso apresentado pelo autor Bruno Ricardo Bioni, no qual uma empresa americana, do mercado varejista, almejando direcionar suas vendas ao público de mulheres grávidas, conseguiu cruzar dados e perceber que esse grupo costumava

[50] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 39.
[51] GALDINO, Natanael. Big Data: Ferramentas e Aplicabilidade. Disponível em: https://www.aedb.br/seget/arquivos/artigos16/472427.pdf. Acesso dia: 26/05/2019.
[52] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 168.

comprar sempre determinados tipos de produtos. A ação da empresa era tão eficaz que conseguiam identificar em qual fase de gestação as mulheres estavam. Assim, a empresa conseguia programar os algoritmos para direcionar publicidades específicas para cada uma[53].

O *Big Data* é considerado por muitos uma solução na atual sociedade da informação. Entretanto, compreendendo seus impactos no âmbito privado e público de seus consumidores, a ausência de uma regulação eficaz pode, na verdade, trazer diversos prejuízos. Para observarmos o grau de lesão ao direito fundamental de proteção de dados, analisemos um caso hipotético.

Um indivíduo, chamado Francisco, mora em uma região com poucos habitantes e uma única drogaria. Todas as vezes em que ele comprava qualquer coisa na farmácia, os dados relacionados a ele ficavam gravados no cadastro de clientes com o seu consentimento. Isso permitia, por exemplo, que ele recebesse descontos em suas próximas compras e planejamento para a farmácia atualizar os tipos de produtos geralmente consumido por seus clientes.

Com o passar do tempo, Francisco passou a comprar diversos medicamentos para pessoas com problemas cardíacos. A farmácia, então, vende os dados de seus clientes para uma empresa de convênio médico, interessada em saber o perfil dos clientes daquela região, sendo um deles o Francisco. A empresa, por meio do processamento desses dados vendidos pela farmácia, analisa a situação de Francisco e aumenta o valor de seu plano médico, devido ao potencial risco para o negócio.

De fato, o aumento do valor do convênio médico de um cliente com mais riscos de saúde não é algo ilícito. Entretanto, a forma de obtenção desses dados foi realizada sem o consentimento do seu titular, ocasionando na violação da sua garantia fundamental. Isso ocorre frequentemente, principalmente pela dificuldade do conhecimento dessa prática. Com isso, outro fator que ameaça os direitos dos consumidores titulares de dados pessoais, é a prática conhecida como *profiling*, que será tratada no próximo subitem.

[53] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 42.

1.2.2 *Profiling*

Na era da *Big Data*, com o exponencial crescimento do uso de *smartphones*, há uma tendência em se colocar todas as informações dos usuários em dados. A reunião desses dados pode constituir um perfil detalhado do indivíduo, visando, preferencialmente a previsão do comportamento dos consumidores[54]. Essa prática é conhecida como *profiling*, e pode causar diversos impactos negativos sobre os cidadãos, uma vez que influenciam no acesso a oportunidades sociais e podem ser utilizados (mesmo que sem a intenção) para práticas discriminatórias.

Com o frequente uso da inteligência artificial, os dados são tratados predominantemente de forma automática com o uso de variadas ferramentas, produzindo informações para a tomada de inúmeras decisões automatizadas. Mesmo que esses dados sejam triviais, ao juntar com outros, podem revelar informações sensíveis do indivíduo[55]. Dessa forma, o perfil gerado pelo tratamento desses dados acaba criando estereótipos que influenciam a vida do seu titular e violam seus direitos de personalidade.

Nesse sentido, os dados anonimizados[56] também podem interferir no livre desenvolvimento da pessoa humana. Por mais que o objetivo desses dados seja para não ser possível identificar uma pessoa e, portanto, manter-se fora da proteção de dados, existem métodos que conseguem reverter o processo de anonimização para que seja possível identificar o seu real titular.

Além disso, os dados anonimizados podem oferecer informações que discriminem uma coletividade ou pessoas singulares, pois a criação de um perfil comportamental pode servir para a exclusão de um indivíduo ou um grupo para determinados fins. Bruno Ricardo Bioni exemplifica muito bem esse fato ao narrar o processo seletivo de determinada empresa, que pretendendo uma maior imparcialidade decidiu realizar um processo anônimo com o critério de escolha daquele que tivesse as características mais parecidas com os funcionários que já

[54] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 111.
[55] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 86.
[56] Conforme o artigo 12, § 2º, da Lei Geral de Proteção de Dados, os dados anonimizados não são considerados dados pessoais, salvo quando existir a possibilidade de serem revertidos e os seus titulares identificados. No mesmo sentido é o entendimento do Regulamento Geral de Proteção de Dados da União Europeia.

integravam a sua equipe[57]. O autor afirma que, muito possivelmente, a decisão automatizada gerada pelo tratamento dos dados anônimos poderia excluir alguns candidatos por questões de etnia, orientação sexual e gênero que fossem diferentes da maioria dos integrantes da empresa.

Situações como essa podem ocorrer em diversos campos a todo momento e, por isso, é imperiosa a construção de uma governança que impeça esse tipo de efeitos nas tomadas de decisão dos cidadãos[58], ao mesmo tempo que permita a continuidade do avanço tecnológico. Como se verá, tamanha é a importância, que tanto a legislação europeia quanto a brasileira tratam diretamente desse assunto.

Contudo, ainda existem desafios no controle de captação e tratamento de dados. Muitas vezes o direito fundamental do cidadão é violado, sem que ele mesmo saiba, ou demore para descobrir. Isso se dá, dentre outros fatores, pela utilização de ferramentas de captação de dados de difícil regulação.

1.3 – A Coleta de Dados Pessoais por meio da Ferramenta de *Cookies*

A sociedade da informação alterou o modo de funcionamento da circulação de riquezas. A inovação tecnológica e o surgimento da internet favoreceram a troca de informações de uma maneira nunca vista. As novidades da rede trouxeram comodidade para a vida cotidiana, e logo tomaram conta de todos os campos da vida em sociedade, seja o trabalho, lazer, relacionamento, entretenimento e outras satisfações pessoais.

Em poucas décadas o mercado virtual cresceu imensamente com o novo fluxo de comunicação, redesenhando a sua estrutura. As pessoas, então, passaram a confiar sua vida privada e íntima nos *softwares* que promovem uma maior facilidade em suas ações cotidianas. Em troca dessas facilidades, dados relativos aos usuários são coletados a todo momento pelas empresas e transformados em informações economicamente relevantes. A possibilidade de prever as ações de cada indivíduo tornou-se um negócio muito lucrativo, não apenas para as empresas que coletam os dados, mas para outras que os compram.

[57] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 79.
[58] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Revista Espaço Jurídico. Vol. 12, nº 2. Joaçaba: Unoesc, 2011, p. 91 – 108.

As chamadas *data brokers* são empresas que coletam informações e dados dos consumidores e os revendem ou compartilham com outras empresas. Geralmente esses dados são utilizados para *marketing* e direcionamento de publicidade, serviços de mitigação de riscos e serviços de busca de pessoas, que permitem a previsão do comportamento dos consumidores[59]. O grande problema é que essa coleta acontece na maioria das vezes sem o consentimento dos usuários ou sem transparência suficiente que mostre qual o objetivo da coleta.

Dessa forma, os direitos de personalidade dos usuários são constantemente violados sem que eles consigam descobrir ou descobrem com imensas dificuldades. Ressalta-se que mesmo informações que não digam muito sobre o indivíduo, quando cruzadas com outras podem revelar dados sensíveis e criar o mencionado *profiling* que, em muitas situações reduzem as oportunidades sociais do sujeito.

Uma das principais ferramentas de coletas de dados, utilizada pela esmagadora maioria das empresas e entidades públicas, é a famosa tecnologia intitulada de *cookies*, que são "marcadores digitais automaticamente inseridos por *websites* visitados, nos discos rígidos do computador, em sua casa ou no local de trabalho, para possibilitar a sua identificação e a memorização de todos os seus movimentos"[60].

Esses dispositivos podem ser benéficos na medida em que lembra usuários para que o sujeito não precise se identificar todas as vezes que entra em determinado site. Além disso, eles podem lembrar os usuários do seu histórico de navegação na internet e indicar interesses de acordo com a sua preferência.

Entretanto, o uso abusivo dessa ferramenta pode comprometer a privacidade do consumidor, tendo em vista a capacidade de monitorar toda as atividades realizadas *online* (e até mesmo *offline*), realizando facilmente um perfil comportamental do consumidor. Essa ameaça à privacidade se agrava ainda mais quando os *cookies* são inseridos em celulares, já que são aparelhos utilizados a todo momento pelos cidadãos.

---

[59] FRAZÃO, Ana. A Industria dos Dados Pessoais e os Data Brokers: Reflexões sobre os riscos da atuação de tais agentes no mercado de dados pessoais. Disponível em: http://anafrazao.com.br/files/publicacoes/2019-03-22-A_industria_dos_dados_pessoais_e_os_data_brokers_Reflexoes_sobre_os_riscos_da_atuacao_de_tais_agente//s_no_mercado_de_dados_pessoais.pdf. Acesso dia: 27/05/2019.

[60] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 101.

Em relação ao método de utilização desses dispositivos, os *cookies* podem ser classificados da seguinte maneira:[61]

a) ***Cookies*** **de Persistência:** Consiste na forma tradicional da utilização desse dispositivo, que fica armazenado no aparelho do usuário por período indeterminados e armazena dados para uso posterior de personalização de serviços, que serão direcionados conforme o perfil de cada usuário. Algumas empresas utilizam esse tipo de *cookies* para armazenar dados não fornecidos diretamente pelo usuário, mas por meio da análise do seu comportamento e perfil de navegação;

b) ***Cookies*** **de Sessão ou Temporários:** Consiste nas mesmas características do anterior, mas a sua duração se limita ao período de navegação em determinado *site*;

c) ***Cookies*** **de Primeira Parte:** Consistem no mecanismo de manutenção da sessão ou captura de informações importantes pertencentes ao domínio que o usuário está acessando diretamente;

d) ***Cookies*** **de Terceiros:** Se originam a partir do relacionamento entre diversos domínios que mantém relação comercial com o *site* visitado. São manipulados por outro provedor que não aquele acessado. Esse tipo de *cookie* pode ser desativado manualmente pelo usuário;

Além dessas classificações, os *cookies* podem ser definidos segundo a sua função[62]:

e) ***Cookies*** **Técnicos:** Permitem que o usuário comprar produtos em um *website*, assistir vídeos, ouvir músicas, ou seja, usufruir os serviços propostos pela plataforma.

f) ***Cookies*** **de Personalização:** Permite que os *websites* funcionem da forma definida pelo usuário.

[61] QUEIROZ, Anderson Apolônio Lira. A Invasão de Privacidade na Internet: um Modelo de Boas Práticas e uma Proposta Interativa de Proteção da Privacidade por Meio dos Cookies. 2011. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011. p. 32.
[62] DUARTE, Vânia Sofia António. Protecção de Dados Pessoais na Internet: O Caso do "Direito a Ser Esquecido". Portugal: Faculdade e Direito da Universidade Nova de Lisboa, 2014, p. 16. https://run.unl.pt/bitstream/10362/17212/1/Duarte_2014.pdf

g) ***Cookies*** **de Comportamentais:** Permite que os responsáveis pelo *site* analisem o comportamento do usuário.

h) ***Cookies*** **de Publicidade:** Permite a criação de um perfil do usuário para direcionamento de publicidade;

Nesse sentido, infere-se que a captação e compartilhamento de dados por meio da ferramenta de *cookies* proporciona benefícios e malefícios aos consumidores. Ao mesmo tempo em que pode ter finalidades úteis e necessárias para facilitar a navegação e permitir o acesso a serviços, eles podem ser utilizados para outras finalidades de transferência e compartilhamento de dados para a criação de *profiling* sem o consentimento ou conhecimento dos usuários. Dessa forma, garantias devem ser proporcionadas para que os direitos de personalidade dos usuários não sejam violados, ao mesmo tempo em que exista uma segurança jurídica para o avanço econômico.

Passada a contextualização teórica da origem e importância da proteção de dados pessoais como um direito de personalidade autônomo, partiremos para a análise de como os ordenamentos jurídicos da União Europeia e do Brasil regulam esse novo direito da personalidade, sobretudo na utilização do mecanismo de *cookies* pelo mercado digital.

CAPÍTULO 2: PROTEÇÃO DE DADOS E REGULAÇÃO DO USO DE *COOKIES* NA UNIÃO EUROPEIA

A União Europeia é a pioneira no que diz respeito à criação de legislação de proteção de dados, tendo em vista que as primeiras regulamentações emanaram de seus membros[63]. Isso se deu principalmente pelo funcionamento do seu mercado interno e o fluxo transfronteiriço de mercadorias, pessoas e informações que acendeu a necessidade de uma legislação equivalente em seus Estados-Membros para a manutenção dos direitos fundamentais na livre circulação de dados[64].

[63] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 96.
[64] CANOTILHO, Mariana; SILVEIRA, Alessandra. Carta dos Direitos Fundamentais da União Europeia Comentada. Coimbra, Portugal: Almedina, 2013, p. 121.

O primeiro grande instrumento comunitário de regulação sobre o tema de proteção de dados surgiu antes mesmo da União Europeia como é conhecida hoje. Esse instrumento, denominado de "Proteção da Privacidade e dos Fluxos Transfronteriços de Dados Pessoais"[65], foi criado pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que, apesar de possuir membros de outros continentes, era formado majoritariamente por países europeus.

A OCDE foi a evolução da Organização Europeia de Cooperação Econômica, organização criada em 1948 com o objetivo de reconstrução da Europa após a Segunda Guerra Mundial, como apoio ao Plano Marshall. Após o ano de 1960, a OECE transformou-se na OCDE, dando um importante início para a posterior criação da União Europeia[66].

Depois da criação desse primeiro regulamento de proteção de dados, a Europa continuou atualizando as suas legislações acerca do tema à medida que a sua estrutura jurídica e política se alterava. Atualmente, as diretivas e regulamentos gerais sobre proteção de dados emanados por ela, além de serem espelhadas no mundo todo, são fundamentais para o fluxo de informações e a economia mundial, devido às exigências para possibilidade de comercialização de produtos e serviços no continente.

Dessa forma, passaremos a analisar a proteção de dados pessoais no Direito Europeu, tendo em vista a sua influência do mundo inteiro. Entretanto, antes de partir para a análise dessas diretivas e regulamentos, faz-se necessário a contextualização do funcionamento da ordem jurídica da comunidade europeia.

2.1 – O Direito na União Europeia

Após a Segunda Guerra Mundial, a Europa sentiu a necessidade de resgatar a ideia de unificação dos Estados, devido ao colapso da economia e estrutura política. O Plano Marshall, necessário para a recuperação econômica do continente no período pós-guerra, foi o grande

[65] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 97.
[66] MARTÍN, Araceli Mangas; NOGUERAS, Diego J. Liñan. *Instituciones Y Derecho de La Unión Europea*. 8ª edição. Espanha, Madrid: Tecnos, 2015, p. 31.

responsável pelo início da união institucional de cooperação e solidariedade política entre os Estados europeus[67].

Em 1947, os apoiadores de uma união entre os Estados europeus, motivados pelo discurso de Churchill no ano anterior[68], reuniram-se no chamado Congresso de Haia representando 24 Estados europeus. Nele, foi decidida a criação da Assembleia Europeia e do "Comitê para a Europa Unida", que visariam[69]:

> - contribuir para criar e exprimir a opinião pública europeia;
> - recomendar as medidas imediatas adequadas ao estabelecimento progressivo, tanto no plano político como no plano econômico, da unidade necessária na Europa;
> - examinar problemas jurídicos e constitucionais colocados pela criação de uma União ou de uma federação, assim como as suas consequências econômicas e sociais;
> - elaborar projetos de instrumentos jurídicos necessários para o efeito;
> - propor a criação de um Tribunal encarregado de assegurar o respeito de uma carta europeia dos direitos humanos.

A iniciativa desse congresso permitiu a criação de importantes organizações e comunidades europeias nos anos futuros, como o Conselho Europeu, criado por meio do Tratado de Londres, em 1949, e a Comunidade Europeia do Carvão e do Aço (CECA), que, embora não houvesse a participação do Reino Unido na sua criação, foi relevante para a evolução da União Europeia. Pelo tratado do CECA, parte dos países europeus limitaram sua soberania ao criar uma autoridade comum, a Alta Autoridade, que iria gerir o setor econômico do carvão e do aço pelos interesses gerais da comunidade, sem receber intervenção de nenhum governo[70].

Em março de 1957, foram assinados, em Roma, outros três tratados criando, dentre outras, a Comunidade Econômica Europeia (CEE), cujo principal objetivo era a criação de um mercado comum por meio de uma união aduaneira. Esse livre mercado abrangia a livre

---

[67] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 35.

[68] Em setembro de 1946, na Universidade de Zurique, o primeiro-ministro britânico Winston Churchill fez um discurso com apelo à unificação da Europa, sobretudo a necessidade de uma reconciliação entre a Alemanha e a França, no qual defendeu: "Devemos criar uma espécie de Estados Unidos da Europa (...). O primeiro passo a dar é criar um Conselho da Europa. Se no início nem todos os Estados europeus quiserem ou puderem aderir à União, cumpre unir, ao menos, os que desejam ou sejam capazes de fazê-lo." Discurso de Churchill, disponível em: http://www.itamaraty.gov.br/pt-BR/sem-categoria/14297-discurso-de-winston-churchill-na-universidade-de-zurique-19-de-setembro-de-1946

[69] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 73.

[70] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 79.

circulação de produtos, pessoas, serviços e capitais. Para que isso fosse possível, foram instituídas políticas comuns para a harmonização das legislações de cada Estado Membro[71].

Por outro lado, no início da década de 1960, o Reino Unido decidiu impulsionar o livre comércio com outros cinco países (Noruega, Dinamarca, Suécia, Áustria e Portugal) e apresentou a criação da Associação Europeia de Comércio Livre (EFTA)[72]. Entretanto, devido ao fracasso dessa organização econômica, o Reino Unido ofereceu o seu pedido oficial de adesão às Comunidades Europeias, que foi negado pela França, dando início a uma crise no planejamento unionista da Europa[73].

Nesse sentido, no ano de 1969, ocorreu a Cimeira de Haia, que teve como principais tópicos a abertura de negociações, com vistas à admissão do Reino Unido, e a concretização da União Econômica e Monetária para solucionar as crises das Comunidades Europeias[74]. Dessa forma, o processo de consolidação e amadurecimento das Comunidades Europeias, que teve como consequência a duplicação dos seus membros, condicionou a assinatura do Tratado de Maastricht (também chamado de Tratado da União Europeia), em 1º de novembro de 1993, responsável pela fundação da chamada União Europeia e lançamento das bases para a moeda única[75].

Nesse contexto, a União Europeia constituiu diversas instituições responsáveis pelos objetivos da União, como o Conselho Europeu, Parlamento Europeu e o Tribunal de Justiça. Entretanto, o Tratado de Maastricht foi considerado como uma fase transitória, necessitando de futuras modificações para a conclusão da integração europeia[76].

Dessa forma, em 1997, o Conselho Europeu realizou o Tratado de Amsterdam, que alargou o âmbito de soberania dos Estados-membros em matérias relacionadas à circulação de pessoas e ampliou as garantias dos direitos fundamentais, como a previsão de sanções ao Estado-membro que violasse o direito de greve e o reconhecimento da competência do Tribunal

[71] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 53.
[72] História da União Europeia, disponível em: https://europa.eu/european-union/about-eu/history/1960-1969/1960_pt
[73] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 85.
[74] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 85.
[75] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 60.
[76] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 114.

de Justiça em matéria de direitos fundamentais[77]. No entanto, as modificações introduzidas por esse tratado foram aquém dos objetivos e finalidades impostas pelo funcionamento da União Europeia[78].

Tendo isso em vista, com o objetivo de sanar as questões deixadas em aberto pelo Tratado de Amsterdam, foi realizado o Tratado de Nice, com entrada em vigor no ano de 2003. O Tratado modificou o peso dos Estados-membro nas votações por maioria qualificada e reduziu as votações por unanimidade. Além disso, outras reformas institucionais foram assinadas para o devido funcionamento da união, levando em consideração a grande ampliação de seus membros e das matérias integradas à sua esfera de atuação[79].

Também foi anunciada a criação de uma nova Conferência Intergovernamental para debater o futuro da União Europeia, tendo como um dos debates o estatuto da Carta dos Direitos Fundamentais da UE. Ademais, foi pensada a criação de uma Constituição Europeia, mas logo foi descartada.

O último tratado assinado foi o Tratado de Lisboa, assinado em 3 de dezembro de 2007, entrando em vigor apenas no final de 2009. O Tratado de Lisboa reformou os tratados em vigor e fez com que a Carta dos Direitos Fundamentais da União Europeia ganhasse vinculação jurídica.

Além disso, o Tratado trouxe significativas mudanças, como: (i) sucedeu a Comunidade Europeia, que deixou de existir; (ii) o exercício da competência da União ficou sujeito à regras equivalentes em todos os domínios políticos; (iii) a União Europeia adquiriu personalidade jurídica, sendo um ente internacional; (iv) a Carta dos Direitos Fundamentais da UE passou a ter força jurídica equivalente aos Tratados; (v) as regras de delimitação da competência dos Estados-membros e da União estão expressamente dispostas nos Tratados, deixando mais clara a separação da esfera de atuação de cada uma; (vi) altera significativamente o funcionamento do quadro orgânico da União Europeia; e (vii) aplicou novas regras de processo de decisão[80].

[77] MARTÍN, Araceli Mangas; NOGUERAS, Diego J. Liñan. *Instituciones Y Derecho de La Unión Europea*. 8ª edição. Espanha, Madrid: Tecnos, 2015, p. 40.
[78] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 61.
[79] Ibidem.
[80] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 81.

Assim, o Tratado de Lisboa impôs importantes mudanças institucionais para garantir os objetivos da União Europeia e lhe conferir uma estrutura unitária. De forma a entender o seu funcionamento, faz-se necessário expor os limites da competência da sua atuação, as funções de suas instituições e em que medida as legislações emanadas pela União afetam os seus Estados-membros.

2.1.1 As atribuições da União Europeia

Os atos jurídicos da União Europeia só podem ser conferidos caso haja uma previsão dos Tratados e outras fontes do direito da União, como a Carta dos Direitos Fundamentais da União Europeia (CDFUE) e os Princípios Gerais da União. Nesse sentido, as suas atribuições são regidas por três princípios: o Princípio da Atribuição, o Princípio da Proporcionalidade e o Princípio da Subsidiariedade.

O primeiro princípio, da Atribuição, vincula e limita a competência da União às atribuições previstas nos Tratados assinados pelos seus Estados-membro. O segundo, da Proporcionalidade, está expressamente previsto no Tratado da União Europeia (TUE) da seguinte forma: "o conteúdo e a forma da ação da União não deve exceder o necessário para alcançar os objetivos do Tratado"[81]. Já o Princípio da Subsidiariedade limita a atuação da União nos domínios em que tanto ela como os Estados-membros podem intervir. Nesses casos, a União só atuará caso a sua intervenção seja mais eficaz do que a ação do Estado-membro.

Os artigos 2º a 6º do Tratado de Funcionamento da União Europeia (TFUE) dispõem acerca das atribuições da União e dos Estados-membro. Em certas áreas, apenas a UE pode legislar, enquanto os membros são limitados apenas à aplicação da legislação criada. Há, contudo, cláusulas de flexibilidade que permite a União intervir em casos definidos. As áreas de competência exclusiva, dentre outras atribuições de celebração de acordos internacionais, são[82]:

- União Aduaneira;

- Regras de matéria concorrencial;

[81] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 323.
[82] EUR-LEX. Tratado de Funcionamento da União Europeia (TFUE), disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso dia: 05/06/2019.

- Política monetária;

- Conservação de recursos biológicos; e

- Comércio comum.

O Tratado também prevê certas áreas de competência partilhada[83]. Nessas áreas, os Estados-membros podem legislar caso a União for omissa sobre o assunto ou decida que não irá legislar. As principais áreas de competência partilhada dizem respeito à defesa dos consumidores, emprego, transporte, energia, segurança e justiça. Além disso, o Tratado determina que nas questões de desenvolvimento tecnológico e ajuda humanitária, a União possui atribuições para desenvolver ações e uma política comum, mas isso não pode impedir os Estados-membros de exercerem a sua própria competência[84].

Dessa forma, diante das suas competências previstas no próprio Tratado de Funcionamento da União Europeia, como por exemplo a defesa do consumidor, e a vinculação jurídica da Carta dos Direitos Fundamentais, a União Europeia pode emanar atos jurídicos que vinculam os seus Estados-membros para a garantia do direito fundamental de proteção de dados pessoais. Portanto, esses atos promovidos pelas suas principais instituições são responsáveis pela regulação de coleta a utilização dos dados dos consumidores no mercado digital, conforme será exposto.

2.1.2 Principais Instituições da União Europeia

O quadro institucional da União está previsto no Tratado da União Europeia assim como no Tratado de Funcionamento da União Europeia, e é composto pelas seguintes instituições:

1) Parlamento Europeu

O Parlamento Europeu está previsto nos artigos 223 ao 234 do TFUE e no artigo 14 do TUE. No que diz respeito às suas competências, o artigo 14 dispõe[85]:

[83] Artigo 4º da TFUE.

[84] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 352.

[85] EUR-LEX. Tratado da União Europeia, disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF. Acesso dia 05/06/2019.

> Artigo 14.o 1. O Parlamento Europeu exerce, juntamente com o Conselho, a função legislativa e a função orçamental. O Parlamento Europeu exerce funções de controlo político e funções consultivas em conformidade com as condições estabelecidas nos Tratados. Compete-lhe eleger o Presidente da Comissão.

Assim, o Parlamento Europeu é o responsável pela produção legislativa da União e pela aplicação de sanções aos Estados-membros que desrespeitarem o direito da UE, além da ter competência para fiscalizar o Conselho e a Comissão. Além disso, após a aquisição de personalidade jurídica pela União, todos os acordos internacionais celebrados que tratam sobre comércio comum ou políticas que sejam abrangidas pelo processo legislativo, devem passar pela análise do Parlamento Europeu antes da entrada em vigor[86].

2) Conselho Europeu

O Conselho Europeu é constituído pelos Chefes de Estado e de Governo dos Estados-membros, e é responsável por impulsionar o desenvolvimento da União, definindo as orientações gerais e prioridades políticas. Essa instituição trata de assuntos complexos que devem ser resolvidos em uma cooperação intergovernamental, como questões de defesa comum e políticas externas. Apesar de tratar sobre temas relevantes, o Conselho Europeu não possui função legislativa. Contudo, pode requerer a elaboração de uma proposta pelo Conselho da União Europeia.

3) Conselho da União Europeia

Conforme o art. 16 da TUE, o Conselho exerce a função legislativa e orçamentária em conjunto com o Parlamento Europeu, possuindo competência para aprovar atos legislativos e o orçamento da União com base nas propostas da Comissão Europeia. Além disso, o Conselho coordena a política econômica e social dos países integrantes da UE e pode celebrar acordos internacionais[87].

4) Comissão Europeia

[86] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 404.
[87] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 416.

A competência da Comissão está prevista no art. 17 da TUE com a seguinte determinação:

> Artigo 17.o 1. A Comissão promove o interesse geral da União e toma as iniciativas adequadas para esse efeito. A Comissão vela pela aplicação dos Tratados, bem como das medidas adotadas pelas instituições por força destes. Controla a aplicação do direito da União, sob a fiscalização do Tribunal de Justiça da União Europeia. A Comissão executa o orçamento e gere os programas. Exerce funções de coordenação, de execução e de gestão em conformidade com as condições estabelecidas nos Tratados. Com exceção da política externa e de segurança comum e dos restantes casos previstos nos Tratados, a Comissão assegura a representação externa da União. Toma a iniciativa da programação anual e plurianual da União com vista à obtenção de acordos interinstitucionais.

A Comissão, portanto, possui o poder de gestão dos serviços e do fundo da União. Além disso, essa instituição pode adotar recomendações, pareceres e atos não legislativos de alcance geral que compelem ou alterem determinados elementos não essenciais do ato legislativo[88].

5) Tribunal de Justiça da União Europeia

O art. 13 da TUE, define a existência de uma instituição jurídica chamada Tribunal de Justiça da União Europeia, que compreende o Tribunal de Justiça, o Tribunal Geral e os Tribunais Especializados, sendo a estrutura jurídica específica da união Europeia[89]. Submetido à garantia do respeito do direito na interpretação dos Tratados[90], o TJUE deve interpretar o direito europeu para que a sua aplicação seja uniforme em todos os países que integram a União.

Nos termos da TFUE, há uma natureza hierárquica entre os Tribunais. Das decisões provindas dos tribunais especializados, cabe recurso ao Tribunal Geral e, por sua vez, as decisões prolatadas pelo TG cabe recurso ao Tribunal de Justiça, que não se confunde com o TJUE. Observa-se que o TJUE é a estrutura jurídica da União que engloba os demais Tribunais. Sendo assim, o Tribunal de Justiça é a instância superior do ordenamento jurídico da União Europeia[91].

Portanto, qualquer cidadão, empresa ou até mesmo Estado-membro e outras instituições podem recorrer ao TJUE caso seja lesado algum direito protegido pelas disposições da União. O recurso pode ser interposto diretamente para o Tribunal Geral ou caso os tribunais nacionais

[88] EUR-LEX, Tratado de Fundação da União Europeia (TFUE), Artigo 290.
[89] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 235.
[90] EUR-LEX, Tratado da União Europeia, artigo 19.
[91] DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011, p. 237.

decidam remeter o caso para a instância superior. O principal objetivo é assegurar a interpretação e aplicação uniforme dos Tratados e demais legislações emanadas pela União.

Além disso, o TJUE possui competência para esclarecer a interpretação dos tribunais nacionais de algum país membro, aplicar a legislação caso o país não o tenha feito, anular atos legislativos que violem os Tratados ou direitos fundamentais, aplicar sanções à instituições europeias que violem direitos e determinar a ação do Parlamento, Conselho ou Comissão em determinadas situações que tenham sido omissos[92].

Dessa forma, o TJUE possui fundamental importância para a uniformização da correta aplicação e interpretação e dos atos legislativos emitidos pelas instituições da União Europeia. Dentre os principais atos jurídicos da União, destacam-se as diretivas e os regulamentos, essenciais para o entendimento da regulação da proteção de dados pessoais na União Europeia, sobretudo na questão da regulação do uso de *cookies* no mercado digital, uma vez que existe diretiva própria sobre o assunto.

2.1.2 Diretivas

A Diretiva é um ato de direito derivado que vincula o Estado-membro quanto ao resultado que deve alcançar, deixando que as instâncias nacionais decidam quanto à forma e aos meios para atingir o resultado esperado pela diretiva[93]. Observa-se, assim, que a diretiva não é direcionada ao indivíduo, mas ao Estado, que deve transpor essa regulação para o seu direito interno. Dessa forma, o cidadão só adquire os direitos e obrigações exigidas pela diretiva após o ato de transposição, pois a aplicação advém de uma norma interna e não da União.

Contudo, apesar de não ser um ato diretamente aplicável aos indivíduos, caso o Estado-membro não realize a transposição no prazo indicado pela diretiva ou a aplique de maneira errada, o Tribunal de Justiça da União Europeia entendeu que ela pode ser aplicada diretamente para que os cidadãos não sejam prejudicados, em comparação aos de outros países da União, por causa da inércia do Estado. Para isso, a diretiva deve ser imperativa, clara e precisa e conferir direitos aos cidadãos[94].

[92] Portal da União Europeia, disponível em: https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_pt. Acesso dia: 05/06/2019.
[93] EUR-LEX, Tratado de Fundação da União Europeia, artigo 288.
[94] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 501.

A diretiva 95/46/CE do Parlamento e do Conselho, de 24 de outubro de 1995, por exemplo, foi transposta para a ordem jurídica portuguesa através da Lei n.º 67/98, de 26/10, que revogou a lei n.º 10/91, de 29/04.

2.1.3 Regulamentos

O regulamento também está previsto no artigo 288 da TFUE. Esse instrumento normativo vinculativo da União possui caráter geral, ou seja, se assemelha com a lei interna dos países membros por força da generalidade, abstração e eficácia *erga omnes*[95]. Portanto, o regulamento não tem destinatário identificável ou determinado, sendo aplicado diretamente aos cidadãos.

Os Estados-membros não podem se negar a obedecer a um regulamento, mesmo que tenham sido contra a sua redação. Nas palavras da autora Ana Maria Guerra Martins[96]:

> A plenitude do efeito obrigatório do regulamento significa que os Estados não podem aplicar o regulamento seletivamente ou de forma incompleta, não podem invocar disposições do seu Direito interno para não aplicarem o regulamento e não podem impedir a execução do regulamento com base no facto de terem expresso sérias reservas quando da sua aprovação.

Nesse sentido, faz-se importante notar que o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) possui grande valor para a proteção dos direitos fundamentais dos cidadãos, impactando todos os vários países da União Europeia de forma padronizada, o que obrigou outros países com interesses comerciais na Europa a criarem suas próprias leis gerais de proteção de dados pessoais, inclusive o Brasil.

Realizado o arcabouço teórico, parte-se para a análise dos atos jurídicos que regulam a proteção de dados pessoais na União Europeia.

2.2 – A Proteção de Dados na União Europeia

Como já exposto, a Europa foi a pioneira na regulação do uso de dados pessoais. Após as recomendações das diretrizes da OCDE, primeiro grande instrumento sobre o tema, a União

[95] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 498.
[96] MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017, p. 498.

Europeia anunciou, em 1980, a Convenção 108, cujo objetivo era a proteção da coleta e tratamento dos dados pessoais[97]. A convenção, também chamada de Convenção de Estrasburgo, definiu suas finalidades no primeiro artigo que dispõe[98]:

> Artigo 1º - Objectivos e finalidades
> A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).

Nota-se que havia uma preocupação com o tratamento automatizado de dados, tendo em vista o desenvolvimento tecnológico que criava mecanismos mais rápidos e práticos para o tratamento. Hoje, na sociedade da informação, esse é um dos principais problemas enfrentados pelos ordenamentos jurídicos para a proteção dos direitos fundamentais, devido, dentre outros problemas, à possibilidade de criação de um *Profiling* dos consumidores gerado pelo tratamento automatizado de seus dados pessoais.

Em 1995, a União Europeia emanou a diretiva 95/46/CE (complementada pela diretiva 2002/58/CE e posteriormente substituída pela RGPD), que era a norma mais moderna à época para a regulação da coleta e tratamento de dados pessoais e ainda possui grande importância na atualidade. Como explicado, a diretiva deve ser transposta para a legislação interna de cada Estado-membro que, devido a diferenças sociais de modelos jurídicos (*common law* e *civil law*), conferiram divergências na legislação de proteção de dados na Europa. Dessa forma, apenas em 2017 todos os países membros se adequaram à essa norma.[99]

A Diretiva 95/46/CE apresentava a preocupação do equilíbrio entre conferir a proteção dos direitos fundamentais dos cidadãos na coleta, armazenamento, tratamento e transmissão de dados pessoais, e garantir o desenvolvimento tecnológico e econômico, fazendo com que a proteção demasiada dos cidadãos não se tornasse um empecilho para o crescimento da economia[100].

---

[97] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 98.
[98] EUR-LEX, Convenção 108, disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso dia 05/06/2019.
[99] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 101.
[100] EUR-LEX. Diretiva 95/46/CE do Parlamento europeu e do Conselho, considerandos 2 e 3, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso dia 05/06/2019.

Nesse sentido, essa regulação assegurou diversos mecanismos que possibilitassem a coleta e tratamento de dados para determinados campos para promover o desenvolvimento na área da biologia, política e economia, prevendo requisitos de coleta, segurança e finalidade para que houvesse exceções às vedações de livre circulação de dados[101]. Além disso, a diretiva reconheceu que o tratamento de dados anonimizados não são protegidos[102], uma vez que impossibilitavam a identificação do indivíduo. Contudo, os dados apenas podem ser considerados anônimos se for impossível a identificação do indivíduo, ou seja, o processo de anonimização não pode ser desfeito ou o cruzamento desses dados com outros não podem possibilitar a identificação do titular.

A diretiva não trata de forma distinta o setor público e privado e nem o tratamento manual ou informatizado dos dados, excluindo do âmbito de proteção apenas o tratamento por pessoas singulares no exercício de atividade exclusivamente pessoal ou doméstico ou do Estado no exercício de defesa e combate a atividades criminais[103].

Em relação à transferência e compartilhamento de dados entre os Estados-membros e países de fora da União Europeia, a diretiva determinou que essa atividade somente poderá ocorrer com países que possuam proteção adequada, nos moldes semelhantes aos da União, conforme o seu artigo 25. Quando o país terceiro não conferir a regulação adequada, a transferência poderá ocorrer quando a entidade que receber os dados se comprometer por meio de cláusula contratual a respeitar os princípios gerais de proteção de dados e oferecer mecanismos suficientes para a garantia[104].

Os principais princípios previstos na legislação, e que tiveram que ser internalizados nas legislações dos Estados-membros, são[105]:

a) **Princípio da Transparência:** Veda a existência de qualquer banco de dados anônimo ou secreto, devendo sempre haver a ciência do titular. Está previsto nos artigos 18 a 21 da diretiva;

[101] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 108.
[102] EUR-LEX. Diretiva 95/46/CE do Parlamento europeu e do Conselho, considerando 26.
[103] CANOTILHO, Mariana; SILVEIRA, Alessandra. Carta dos Direitos Fundamentais da União Europeia Comentada. Coimbra, Portugal: Almedina, 2013, p. 122.
[104] Ibidem, p. 127.
[105] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 108.

b) Princípio da Finalidade: Determina que todo dado coletado deve ser armazenado, tratado e divulgado para o fim informado ao titular, não podendo haver nenhum desvio de finalidade sem a ciência do titular. Esse princípio está previsto no artigo 6º;

c) Princípio da Necessidade: Também previsto no artigo 6º, esse princípio está ligado ao princípio da finalidade e limita a coleta de dados ao mínimo indispensável para o seu fim;

d) Princípio da Exatidão: Exige que os dados sejam coletados e tratados da maneira exata, completa e atualizada, permitindo que os titulares exijam a atualização ou correção de determinado dado. Está previsto no artigo 6º e 12 da diretiva.

e) Princípio do Consentimento: Com base na autodeterminação informativa, a diretiva determina, em se artigo 7º, que a coleta e o tratamento de dados pessoais só podem ocorrer com o consentimento do seu titular, que deve ser livre, consciente, específico e inequívoco[106]. Entretanto, o princípio não é absoluto, havendo certas exceções também previstas no próprio artigo 7º[107].

Os princípios acima elencados foram tão relevantes para o ordenamento europeu que perduraram até a legislação mais recente acerca da proteção de dados pessoais na União Europeia. O Regulamento Geral de Proteção de Dados Pessoais (RGPD), que substituiu a diretiva 95/46/CE, abrangeu esses princípios e os conferiu força normativa em todos os Estados-

[106] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 115.

[107] Artigo 7.

Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se:

a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou

b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou

c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou

d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa; ou

e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou

f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º.

membros, sem a necessidade de transposição para o ordenamento interno de cada país, uma vez que, como explicado, os regulamentos são diretamente aplicáveis e possuem efeito *erga omnes*.

Faz-se relevante observar que os dados sensíveis previstos na RGPD também foram tratados pela diretiva 95/46/CE. Essa legislação praticamente vedava todo o tratamento de dados sensíveis sem o consentimento dos seus titulares, mas aceitava determinadas exceções por interesse social maior ou do próprio indivíduo[108]. Nesse sentido:

> Artigo 8º
> Tratamento de certas Categorias Específicas de Dados
> 1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.
> 2. O n" 1 não se aplica quando:
> a) A pessoa em causa tiver dado o seu consentimento explícito para esse tratamento, salvo se a legislação do Estado-membro estabelecer que a proibição referida no n" 1 não pode ser retirada pelo consentimento da pessoa em causa; ou
> b) O tratamento for necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho, desde que o mesmo seja autorizado por legislação nacional que estabeleça garantias adequadas; ou
> c) O tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento; ou
> d) O tratamento for efectuado, no âmbito das suas actividades legítimas e com as garantias adequadas, por uma fundação, uma associação ou qualquer outro organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, na condição de o tratamento dizer unicamente respeito aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem o consentimento das pessoas em causa ; ou
> e) O tratamento disser respeito a dados manifestamente tornados públicos pela pessoa em causa ou for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial.
> 3. O n " 1 não se aplica quando o tratamento dos dados for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços da saúde e quando o tratamento desses dados for efectuado por um profissional da saúde obrigado ao segredo profissional pelo direito nacional ou por regras estabelecidas pelos organismos nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente.
> 4. Sob reserva de serem prestadas as garantias adequadas, os Estados-membros poderão estabelecer, por motivos de interesse público importante, outras derrogações para além das previstas no n? 2, quer através de disposições legislativas nacionais, quer por decisão da autoridade de controlo referida no artigo 28"
> 5. O tratamento de dados relativos a infracções, condenações penais ou medidas de segurança só poderá ser efectuado sob o controlo das autoridades públicas ou se o direito nacional estabelecer garantias adequadas e específicas, sob reserva das derrogações que poderão ser concedidas pelo Estado-membro com base em disposições nacionais que prevejam garantias específicas e adequadas. Contudo, o registo completo das condenações penais só pode ser mantido sob o controlo das autoridades públicas. Os Estados-membros podem estabelecer que o tratamento de

[108] CANOTILHO, Mariana; SILVEIRA, Alessandra. Carta dos Direitos Fundamentais da União Europeia Comentada. Coimbra, Portugal: Almedina, 2013, p. 125.

> dados relativos a sanções administrativas ou decisões cíveis fique igualmente sujeito ao controlo das autoridades públicas.
> 6. As derrogações ao n° 1 prevista nos n "s 4 e 5 serão notificadas à Comissão.
> 7. Cabe aos Estados-membros determinar as condições em que um número nacional de identificação ou qualquer outro elemento de identificação de aplicação geral poderá ser objecto de tratamento[109].

Além das inovações trazidas para a proteção de dados, a Diretiva 1995/46/CE dispôs acerca da criação de um Grupo de proteção de dados pessoais que ficasse responsável por formular recomendações e pareceres para aconselhar a Comissão sobre quaisquer projetos de alteração da diretiva e analisar questões relativas à aplicação das disposições nacionais da diretiva, com o objetivo de garantir uma aplicação uniforme entre os Estados-membros. As suas atribuições foram dispostas no artigo 30 da seguinte forma:

> Artigo 30
> 1. O grupo tem por atribuições:
> a) Analisar quaisquer questões relativas à aplicação das disposições nacionais tomadas nos termos da presente directiva , com vista a contribuir para a sua aplicação uniforme;
> b) Dar parecer à Comissão sobre o nível de protecção na Comunidade e nos países terceiros;
> c) Aconselhar a Comissão sobre quaisquer projectos de alteração da presente directiva ou sobre quaisquer projectos de medidas adicionais ou específicas a tomar para proteger os direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como sobre quaisquer outros projectos de medidas comunitárias com incidência sobre esses direitos e liberdades;
> d) Dar parecer sobre os códigos de conduta elaborados a nível comunitário.
> 2. Se o grupo verificar que surgem divergências susceptíveis de prejudicar a equivalência da protecção das pessoas no que diz respeito ao tratamento de dados pessoais na Comunidade entre a legislação ou a prática dos Estados -membros, informará desse facto a Comissão.
> 3. O grupo pode, por sua própria iniciativa, formular recomendações sobre quaisquer questões relativas à protecção das pessoas no que diz respeito ao tratamento de dados pessoais na Comunidade.
> 4. Os pareceres e recomendações do grupo serão transmitidos à Comissão e ao comité referido no artigo 31 "
> 5. A Comissão informará o grupo do seguimento que deu aos seus pareceres e recomendações. Para o efeito, elaborará um relatório que será igualmente enviado ao Parlamento Europeu e ao Conselho. O relatório será publicado.
> 6. O grupo elaborará um relatório anual sobre a situação da protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais na Comunidade e nos países terceiros, que será comunicado à Comissão, ao Parlamento Europeu e ao Conselho. O relatório será publicado.

O grupo ficou conhecido como Grupo do Artigo 29[110] e lidou com diversas questões relacionadas a proteção de dados e privacidade até a data de aplicação da RGPD (25 de maio de 2018). Suas recomendações foram relevantes para a compreensão dos dispositivos da diretiva. Inclusive, já previu a necessidade da prestação de informação acerca do uso de *cookies.*

[109] EUR-LEX. Diretiva 95/46/CE do Parlamento europeu e do Conselho, artigo 8º.
[110] Pag 250 do Bruno (rodapé 175)

Por fim, a diretiva também teve fundamental importância ao determinar a impossibilidade de decisões individuais automatizadas que levem em consideração os dados coletados e que afetassem a esfera jurídica ou econômica do titular, admitindo casos excepcionais que houvesse previsão legal[111]. Além disso, previu a criação de uma autoridade exclusiva e independente que fiscalizasse e aplicasse sanções caso a legislação não fosse cumprida. Essas determinações foram tão relevantes que a própria RGPD as mantiveram.

Além da diretiva 95/46/CE, outra diretiva de extrema relevância e que ainda está em vigor é a diretiva 2002/58/CE, que, dentre outros fatores, compreendeu a importância da regulação do uso de ferramentas de coleta, transferência e tratamento de dados, como a denominada "testemunho de conexão", mais conhecido por Cookies.

2.2.1 Diretiva 2002/58/CE

A Diretiva 2002/58/CE trata da proteção de dados pessoais e a proteção da privacidade na área das comunicações eletrônicas e internet, aplicando os princípios estabelecidos na Diretiva 95/46/CE e na CDFUE como regras para o setor de comunicação eletrônico. Os seus considerandos retratam muito bem o objetivo de tratamento no ambiente eletrônico, prevendo proposições e meios específicos de controle, como a conservação de dados para fins de faturamento dos serviços de conexão[112] e a utilização de cookies, conforme o considerando 25[113]:

> Todavia, esses dispositivos, por exemplo os denominados testemunhos de conexão («cookies»), podem ser um instrumento legítimo e útil, nomeadamente na análise da eficácia da concepção e publicidade do sítio web, e para verificar a identidade dos utilizadores que procedem a transacções em linha. Sempre que esses dispositivos, por exemplo os testemunhos de conexão («cookies»), se destinem a um fim legítimo, como por exemplo a facilitar a prestação de serviços de informação, a sua utilização deverá ser autorizada, na condição de que sejam fornecidas aos utilizadores informações claras e precisas, em conformidade com a Directiva 95/46/CE, acerca da finalidade dos testemunhos de conexão («cookies») ou dos dispositivos análogos por forma a assegurar que os utilizadores tenham conhecimento das informações colocadas no equipamento terminal que utilizam. Os utilizadores deveriam ter a oportunidade de recusarem que um testemunho de conexão («cookie») ou um dispositivo análogo seja armazenado no seu equipamento terminal. Tal é particularmente importante nos casos em que outros utilizadores para além do próprio têm acesso ao equipamento terminal e, consequentemente, a quaisquer dados que

[111] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 120.
[112] Do artigo daquele brother.
[113] EUR-LEX. Diretiva 2002/58/CE do Parlamento europeu e do Conselho, Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN. Acesso dia: 05/06/2019

> contenham informações sensíveis sobre a privacidade armazenadas no referido equipamento. A informação e o direito a recusar poderão ser propostos uma vez em relação aos diversos dispositivos a instalar no equipamento terminal do utente durante a mesma ligação e deverá também contemplar quaisquer outras futuras utilizações do dispositivo durante posteriores ligações. As modalidades para prestar as informações, proporcionar o direito de recusar ou pedir consentimento deverão ser tão conviviais quanto possível. O acesso ao conteúdo de um sítio web específico pode ainda depender da aceitação, com conhecimento de causa, de um testemunho de conexão («cookie») ou dispositivo análogo, caso seja utilizado para um fim legítimo.

Na versão original, o artigo 5º, nº 3, da diretiva permitia que as informações e dados fossem armazenados pelas redes de comunicação eletrônica ou captados no equipamento[114] do utilizador/consumidor com a condição de serem prestadas informações claras e completas ao titular acerca da utilização dos dados captados e a finalidade do tratamento, garantindo o direito de recusa do tratamento ao cidadão a qualquer tempo. Assim, alguns países interpretaram que não era necessário um consentimento prévio para a aplicação dos *cookies* nos equipamentos dos consumidores.

Contudo, com o objetivo de garantir uma maior proteção à autodeterminação informativa do cidadão, a Diretiva 2009/135/CE modificou o disposto no artigo 5º, nº 3, da Diretiva 2002/58/CE, que passou a exigir a prévia obtenção do consentimento do titular para a utilização de *cookies*, alterando significativamente a forma de utilização dessa ferramenta pelas plataformas digitais[115].

Nesse contexto, apesar das alterações propostas por essa diretiva, a Diretiva 1995/46/CE continuou sendo aplicada (até a sua revogação pela RGPD), nos termos do considerando nº 10[116], exceto nas disposições expressamente previstas pela Diretiva

[114] O considerando 24 da Diretiva 2002/58/CE, considera os equipamentos (computadores, celulares, etc.) dos cidadãos parte integrante da sai vida privada, ao dispor que "o equipamento terminal dos utilizadores de redes de comunicações electrónicas e todas as informações armazenadas nesse equipamento constituem parte integrante da esfera privada dos utilizadores e devem ser protegidos ao abrigo da Convenção Europeia para a Protecção dos Direitos Humanos e das Liberdades Fundamentais. Os denominados «gráficos espiões», «programas-espiões», («spyware»), «gráficos-espiões» («web bugs») e «identificadores ocultos» («hidden identifiers») e outros dispositivos análogos podem entrar nos terminais dos utilizadores sem o seu conhecimento a fim de obter acesso a informações, armazenar informações escondidas ou permitir a rastreabilidade das actividades do utilizador e podem constituir uma grave intrusão na privacidade desses utilizadores. A utilização desses dispositivos deverá ser autorizada unicamente para fins legítimos, com o conhecimento dos utilizadores em causa." Isso confirma o interesse da União Europeia em proteger a vida privada e os dados pessoais dos seus cidadãos, considerando os equipamentos utilizados no setor de comunicação eletrônica como uma extensão da vida privada do cidadão.

[115] FONTAÍNHAS, Emília Golim; ANDRADE, Francisco; AMLEIDA, José Bacelar. Do Consentimento para a Utilização de Testemunhos de Conexão (cookies). Portugal: Scientia Iuridica, Tomo LXV nº 341, 2016, p. 182.

[116] Nos termos do considerando 10 da Diretiva 2002/58/CE, "No sector das comunicações electrónicas, é aplicável a Directiva 95/46/CE, especialmente no que se refere a todas as questões relacionadas com a protecção dos direitos e liberdades fundamentais não abrangidos especificamente pelas disposições da presente directiva,

2002/58/CE, uma vez que, segundo o critério da especialidade, a lei específica prevalece sobre a lei geral. Dessa forma, as disposições acerca dos princípios, direitos do titular, confidencialidade e segurança da coleta, tratamento e transferência de dados, ainda forma aplicados por muito tempo[117], até a entrada em vigor da RGPD no ano de 2018. Entretanto, conforme será exposto mais à frente, os princípios da Diretiva 95/46/CE e grande parte das suas disposições foram englobadas pelo Regulamento Geral de Proteção de Dados, vigorando até os dias atuais.

A ferramenta de *cookies* é um tratamento invisível de dados, o que o conferiu uma regulação própria na União Europeia. Como exposto, o princípio basilar do uso legítimo de *cookies* é o consentimento prévio do consumidor cidadão para a sua aplicação no equipamento digital. Desde a Diretiva 95/56/CE, a forma de consentimento sofreu alterações e implicou consequências para o uso dessa ferramenta pelas plataformas digitais. Nesse sentido, para que se possa compreender o modo de regulação dessa ferramenta na União Europeia, deve-se analisar os requisitos relativos ao consentimento.

A) O Consentimento do Consumidor para a Utilização de Cookies

O consentimento como um dos fundamentos de legitimidade para a coleta e tratamento de dados pessoais surgiu na Diretiva 95/46/CE, que o compreendeu como[118]/[119]:

incluindo as obrigações que incumbem à entidade que exerce o controlo e os direitos das pessoas singulares. A Directiva 95/46/CE é aplicável aos serviços de comunicações não acessíveis ao público."

[117] FONTAÍNHAS, Emília Golim; ANDRADE, Francisco; AMLEIDA, José Bacelar. Do Consentimento para a Utilização de Testemunhos de Conexão (cookies). Portugal: Scientia Iuridica, Tomo LXV nº 341, 2016, p. 182.

[118] EUR-LEX. Diretiva 95/46/CE do Parlamento europeu e do Conselho, artigo 2º, alínea *f*.

[119] A Regulação Geral de Proteção de Dados (GDPR), que substituiu a referida diretiva, abarcou o mesmo conceito de consentimento, deixando-o ainda mais claro. Assim está disposto em seu considerando 32:

"(32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido".

> h) « Consentimento da pessoa em causa », qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento.

Somados a isso, o novo disposto na Diretiva 2002/56/CE, com a atualização realizada pela Diretiva 2009/136/CE, determinou a necessidade de consentimento prévio para a coleta, armazenamento e tratamento de dados ou a possibilidade de acesso à informações já presentes no equipamento do usuário, devendo, ainda, ser declarado a finalidade do processamento, segundo o disposto no art. 5º, nº 3, com a seguinte redação[120]:

> «3. Os EstadosMembros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efectuar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»;

O consentimento prévio, prestado com base em informações claras e completas, livre, específico acerca da finalidade e inequívoco, e a possibilidade de revogação desse consentimento a qualquer tempo são os principais fundamentos de legitimidade para a utilização da ferramenta de *cookies* na União Europeia (mas não os únicos). Caso, por exemplo, o *cookie* utilizado sirva para diversas finalidades, deve haver informações claras e completas acerca de cada uma para que o titular possa exercer o livre consentimento.

A necessidade em conferir ao cidadão o consentimento prévio para a aplicação do "testemunho de conexão" deve-se ao fato de que a sua utilização é discreta e o eventual dano causado não é prontamente percebido pelo titular. Antes dessa legislação, o *website* visitado poderia coletar dados e informações do indivíduo e até mesmo rastreá-lo sem que ele fosse notificado por isso ou tivesse algum conhecimento.

Dessa forma, o elevado risco dessa atividade para a violação de dados motivou o legislador europeu a exigir o consentimento prévio como requisito legal do uso de *cookies* para que o consumidor cidadão tivesse o conhecimento da existência dessa ferramenta discreta de coleta de dados e pudesse decidir sobre a sua utilização[121].

---

[120] EUR-LEX. 2002/56/CE do Parlamento europeu e do Conselho, artigo 5º, nº 3, após a Diretiva 2009/136/CE (grifou-se).

[121] FONTAÍNHAS, Emília Golim; ANDRADE, Francisco; AMLEIDA, José Bacelar. Do Consentimento para a Utilização de Testemunhos de Conexão (cookies). Portugal: Scientia Iuridica, Tomo LXV nº 341, 2016, p. 186.

Ainda, a exigência de oferecer informações claras e exatas acerca da finalidade do tratamento de dados permite uma maior oportunidade para que o titular saiba quando os seus dados pessoais estão sendo utilizados de forma abusiva ou equivocada, algo praticamente impossível quando não há nenhuma evidência da utilização desse tipo de ferramenta.

Nesse sentido, a informação de quando o *software* pode receber, armazenar e transferir dados por meio de um *cookie* e o seu objetivo e sua duração, devendo, ainda, a mensagem transmitida pelo operador ser em uma linguagem clara e compreensível de nível geral[122], oferece não apenas uma proteção direta dos direitos fundamentais do cidadão, mas a possibilidade de reparação do direito violado pela tutela jurisdicional do Estado. Ou seja, além da possibilidade de evitar que as empresas violem os direitos fundamentais à privacidade e à proteção de dados do indivíduo, caso isso ocorra, o cidadão encontra uma maior chance de reconhecimento dessa violação e pode exigir a reparação do dano pela empresa que o causou. Contudo, como se verá ao longo do presente trabalho, basear a proteção de dados pessoais apenas no consentimento do cidadão pode não ser a maneira ideal para a solução do problema, visto que o consentimento nem sempre proporciona ao cidadão uma real emancipação da sua autodeterminação informacional.

Além disso, o entendimento acerca do consentimento não foi uniforme em todos os Estados-membros da União. Como as diretivas não possuem eficácia imediata e precisam ser transpostas para a legislação interna de cada país, as autoridades nacionais interpretaram de forma divergente a aplicação do 5º, nº 3 da Diretiva 2002/56/CE. Além disso, outros dispositivos foram distintamente recepcionados pelos países da União, motivando o Grupo do Artigo 29 a emanar diversos pareceres para tentar unificar a interpretação das diretivas.

A Alemanha e o Reino Unido, por exemplo, tiveram o entendimento de que o consentimento exigido no novo nº 3 do artigo 5º deveria, na realidade, ser exercido como direito de recusa do armazenamento de dados ou do posterior acesso[123]. Isso se deve pela desconformidade entre as versões do dispositivo nas diversas línguas da União[124]. Nesse sentido, por meio do parecer 2/2010, o Grupo do Artigo 29 defendeu que o consentimento deve ser prévio, ou seja, obtido antes da instalação dos *cookies* no equipamento do usuário.

[122] Ibidem.
[123] FONTAÍNHAS, Emília Golim; ANDRADE, Francisco; AMLEIDA, José Bacelar. Do Consentimento para a Utilização de Testemunhos de Conexão (cookies). Portugal: Scientia Iuridica, Tomo LXV nº 341, 2016, p. 191
[124] Ibidem.

Outra divergência se deu em relação ao consentimento inequívoco ao qual se refere a alínea *a* do artigo 7 da Diretiva 95/46/CE. Seguindo o raciocínio no artigo 2º da referida diretiva, consentimento é "qualquer manifestação de vontade, livre, específica e informada", pela qual o titular aceita que seus dados pessoais sejam objeto de tratamento. Essa definição gerou interpretações desiguais, tendo em vista o elevado grau de abstração do que pode ser considerado uma manifestação de vontade.

Diante disso, o Grupo do Artigo 29 declarou sua opinião de que o consentimento tácito não era suficiente para se demonstrar inequívoco, devendo ser realizado explicitamente[125]. Contudo, como não há nenhuma previsão, na diretiva, de que o consentimento para o tratamento de dados pessoais genéricos deve ser explícito, alguns países compreenderam ser possível o consentimento tácito.

Por fim, cabe ressaltar que o consentimento para o uso de *cookies* pode ser mitigado em determinadas situações. O próprio dispositivo[126] que exige o consentimento prévio para que o "armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador" sejam permitidos, reconhece que o consentimento pode sofrer exceções em caso de armazenamento técnico ou acesso com a única finalidade de realizar transmissão de uma comunicação através de uma rede de comunicações eletrônicas, "ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador". Portanto, a exceção do consentimento depende exclusivamente da finalidade do *cookie* ou do pedido realizado expressamente pelo titular que exija o uso do *cookie* para que o serviço solicitado possa ser concluído.

Nesse contexto, a Comissão Europeia possui um "Manual de Internet Oficial"[127] que indica quais *cookies* são claramente isentos de consentimento, sendo:

a) ***Cookies*** **Inseridos pelo Usuário:** São aqueles que rastreiam a entrada do usuário ao preencher formulários, adicionar carrinho de compras, etc. São *cookies* temporários que duram durante a sessão ou limitados a algumas horas após;

[125] Ibidem.
[126] EUR-LEX. 2002/56/CE do Parlamento europeu e do Conselho, artigo 5º, nº 3, após a ratificação pela Diretiva 2009/136/CE.
[127] IRWIN, Luke. *How the GDPR Affects Cookie Policies.* Disponível em: https://www.itgovernance.eu/blog/en/how-the-gdpr-affects-cookie-policies. Acesso dia 15/06/2019.

b) ***Cookies*** **de Autenticação:** Identificam o usuário logado durante a sessão;

c) ***Cookies*** **de Segurança:** Servem para detectar abusos de tentativa de autenticação com várias falhas.

d) ***Cookies*** **de Conteúdo Multimídia:** Servem para armazenar dados técnicos para reproduzir música ou vídeo durante a sessão;

e) ***Cookies*** **de Balanceamento de Carga:** Ajudam a distribuir as solicitações do servidor de maneira uniforme para evitar problemas de conexão;

f) ***Cookies*** **de Personalização de Interface:** Personaliza opções de idioma ou fonte. Tem a duração da sessão ou poucas horas depois.

B) Interesse Legítimo na Diretiva 95/46/CE

Conforme o artigo 7º da Diretiva 95/46/CE, o consentimento não é o único fundamento de legitimidade para o tratamento de dados. Está previsto, na alínea *f* do referido artigo, que se "o tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º" o tratamento de dados será legítimo. Entretanto, a diretiva europeia não dá detalhes sobre o que seriam os interesses legítimos e como seriam aplicados, permitindo uma extensa linha interpretativa para as legislações internas.

Nesse sentido, o autor Bruno Ricardo Bioni compreende que:

> Como resultado, ao longo da vigência da diretiva, notou-se, negativamente: a) a ausência de uma aplicação harmônica e consistente de tal base legal entre os países do bloco econômico europeu; e b) o risco de o âmbito de aplicação das outras bases legais ser esvaziado, na medida em que o legítimo interesse poderia ser visto como aquela menos restritiva que as demais[128].

[128] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p 250.

Dessa forma, um consumidor que permitiu a utilização de *cookie* para determinada finalidade, poderia ter o seu livre consentimento violado caso o operador utilizasse os seus dados e informações para outro fim que não aquele acordado, sob a justificativa de interesse legítimo, sem que fosse possível a aplicação de uma limitação uniforme a esse dispositivo nos países da União. Haveria, portanto, uma possibilidade de contornar direitos e princípios previstos pela própria diretiva.

C) Tratamento de Dados por meio de Cookie de Terceiros

O responsável pelo tratamento de dados possui a obrigação de fornecer informações claras e completas acerca da coleta e uso de dados do titular. No caso de *cookies* de terceiros, nos quais outra empresa aplica a ferramenta por meio de outro *website*, a responsabilidade dessa obrigação recai sobre a empresa terceira, nos termos da diretiva 95/46/CE. Seria ela, também, a responsável por qualquer dano causado ao titular dos dados pessoais por eventual violação.

Entretanto, o Grupo do Artigo 29[129] formulou a opinião de que os sites que alojam os *cookies* de terceiros são corresponsáveis pelos *cookies* instalados, na medida da sua participação. Segundo o entendimento, o responsável é aquele agente que possa tomar as decisões sobre como ocorrerá o tratamento de dados e com qual finalidade, não sendo necessariamente aquele que coleta diretamente os dados dos titulares[130].

2.2.2 Regulamento Geral de Proteção de Dados da União Europeia (RGPD)

Como observado, as diretivas de proteção de dados tiveram papel fundamental para a garantia dos direitos fundamentais à privacidade e proteção de dados dos cidadãos da União Europeia. Contudo, os diversos conflitos decorrentes das diferentes interpretações e aplicações nas legislações internas dos Estados-membros e os avanços na tecnologia de coleta e tratamento de dados exigiram que o Parlamento Europeu e o Conselho promulgassem uma nova norma de aplicação imediata e uniforme. Nesse sentido, em abril de 2016 foi publicado o Regulamento

[129] Parecer 2/2010.
[130] MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo, Thomson Reuters, 2018, p. 115.

Geral de Proteção de Dados que viria a substituir a Diretiva 95/46/CE em maio de 2018, ao entrar em vigor.

O novo ato normativo foi necessário para padronizar e resguardar de forma mais eficiente a privacidade, gerando condições mais igualitárias para o tratamento de dados e uma maior segurança jurídica entre os Estados-membros. A importância dessa nova norma em relação às diretivas pode ser observada logo na diferença de aplicação entre as Diretivas e os Regulamentos, no sentido em que

> A primeira tem apenas o condão de direcionar, mas permitindo que cada Estado possua discricionariedade de adaptar à sua realidade nacional o direcionamento emanado pelo Parlamento, tendo apenas a condicionante de manter os princípios estabelecidos. Enquanto o segundo tem força vinculativa, sendo um ato legislativo vinculativo e aplicável em todos os seus elementos diretamente aos países-membros da EU, ou seja, trata-se de uma norma impositiva que independe de qualquer outro ato estatal para a sua eficácia no direito interno[131].

Apesar da nova regulação trazer mudanças significativas no ordenamento da União, os princípios definidos na Diretiva 95/46/CE foram recepcionados e permanecem válidos. Como se pode observar no considerando nº 9[132] do RGPD, os princípios e objetivos da diretiva não foram capazes de evitar a fragmentação da proteção de dados no nível da União devido às disparidades na execução e aplicação da diretiva. Dessa forma, além dos objetivos trazidos na diretiva, o regulamento tem a finalidade de tornar equivalente o nível de proteção de dados em todo o território da União dando, ainda, espaço para que os países integrantes possam especificar suas regras em situações específicas de tratamento. Assim está disposto no considerando nº 10:

> (10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados

[131] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 123.

[132] O considerando nº 9 dispõe: "Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE".

> pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

Desse modo, além de promover a uniformidade da proteção de dados pessoais, o regulamento permite a liberdade de normas internas específicas acerca do tratamento dos dados, conforme conveniência, realidade e interesse, desde que não contrariem os princípios e regras gerais do regulamento, que independem de nacionalidade para serem respeitados[133]. Entretanto, o RGPD reconhece que o direito a proteção de dados pessoais não é absoluto e deve ser considerado e analisado de acordo com a sua função na sociedade, devendo ser equilibrado com os demais direitos fundamentais por meio do princípio da proporcionalidade[134].

O Regulamento seguiu uma linha expansionista sobre o que pode ser considerado dados pessoais. Na nova era da informação, essa expansão inclui fotos, áudios, endereço de IP e outros elementos como dado pessoal de um indivíduo. O Regulamento também dispõe expressamente acerca da ferramenta de *cookies* no considerando nº 30:

> (30) As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.

[133] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 124.

[134] Nesse sentido, o considerando nº 4 dispõe que "o tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística".

Ao considerar os *cookies* como dado pessoal, o Regulamento os torna sujeitos às suas diretrizes, exigindo uma adaptação da Diretiva 2002/58/CE[135]. Cabe ressaltar que a utilização de *cookies* ainda é regulada por essa Diretiva, mas como o Regulamento substituiu a Diretiva 95/46/CE, a "Lei de *cookies*" deve seguir os princípios e regras gerais do RGPD. Nesse sentido:

> Artigo 95.o Relação com a Diretiva 2002/58/CE
> O presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva 2002/58/CE.

A) O Consentimento no RGPD

Como mencionado, o RGPD manteve os princípios e grande parte dos conceitos da diretiva que substituiu. Nesse contexto, o nº 11 do seu artigo 4º adjetiva o consentimento da seguinte maneira:

> Art. 4º. 11) «Consentimento» do titular dos dados: uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

Como se pode notar, ainda são utilizados os adjetivos "livre", "específica", "informada" e "explícita". Além disso, o considerando nº 32 ainda afirma que o consentimento deverá ser dado mediante ato positivo e claro que indique a manifestação livre, específica, informada e inequívoca de que o titular consente com o tratamento de dados. Observa-se, portanto, um fator relevante para a padronização das legislações dos países integrantes da União.

Ao exigir um "ato positivo claro" e inequívoco da manifestação, o Regulamento indica a necessidade de um consentimento "mediante declaração escrita, inclusive em formato eletrônico ou declaração oral", como expõe a própria norma. Isso quer dizer que o consentimento prévio exigido pela Diretiva 2002/58/CE não pode ser considerado por meio de

[135] Nesse sentido o considerando nº 173 do RGPD prevê: "O presente regulamento deverá aplicar-se a todas as matérias relacionadas com a defesa dos direitos e das liberdades fundamentais em relação ao tratamento de dados pessoais, não sujeitas a obrigações específicas com o mesmo objetivo, enunciadas na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho (2), incluindo as obrigações que incumbem ao responsável pelo tratamento e os direitos das pessoas singulares. A fim de clarificar a relação entre o presente regulamento e a Diretiva 2002/58/CE, esta última deverá ser alterada em conformidade. Uma vez adotado o presente regulamento, a Diretiva 2002/58/CE deverá ser revista, em especial a fim de assegurar a coerência com o presente regulamento."

uma omissão no sentido de não se opor ou limitado ao simples "quem cala consente". Dessa forma, o consentimento tácito não deve ser considerado válido.

O Regulamento também exige que o responsável pelo tratamento de dados informe o titular acerca da sua identidade e as finalidades do tratamento, bem como os destinatários dos dados e o fundamento jurídico do tratamento. Além disso, o titular deve ser informado da existência de decisões automatizadas, incluindo a definição de perfis e dos perigos daí advindos. Outras informações relevantes também são exigidas no artigo 13 do RGPD, como o prazo da conservação dos dados ou os critérios utilizados para defini-lo.

O titular deve, ainda, poder retirar o seu consentimento a todo o tempo, devendo ser tão fácil de retirar quanto de dar, conforme o artigo 7º[136]. Se o titular não puder recusar ou retirar o consentimento sem ser prejudicado, o consentimento não será considerado livre e a utilização da ferramenta de *cookies* será ilegítima (considerando nº 43). O consentimento também não é considerado livre se não for possível individualizá-lo para diferentes tratamentos de dados, mesmo que sejam adequados[137].

Sempre que os dados forem utilizados para outros fins que aqueles informados, ele deve fornecer as informações aos titulares. Conforme o princípio da transparência, previsto no considerando nº 58, as informações devem ser de fácil acesso e compreensão, bem como formuladas em uma linguagem clara e simples e que se recorra à visualização sempre que for adequado.

Assim, o consentimento ficou mais claro e definido com a GDPR. Para o uso legítimo da ferramenta de *cookies*, portanto, deve haver um consentimento prévio e explícito, com

---

[136] Artigo 7.
Condições aplicáveis ao consentimento
1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.
4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

[137] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 135.

informações exatas de fácil entendimento e a exposição das finalidades da aplicação da ferramenta, bem como a opção de recusar o consentimento a qualquer tempo. O grande problema para a limitação da dualidade entre "permitir" e "não permitir" reside principalmente em dois fatos:

(i) a exclusão do indivíduo do mercado, uma vez que muitas empresas podem vincular os *cookies* a um bloqueio prévio que não permite o acesso ao serviço daquele usuário que não aceitou; e

(ii) o consentimento prévio e expresso para todas as finalidades do eventual *cookie* utilizado pode bombardear o usuário de avisos de instalação de *cookies*, tornando a navegação maçante e inviabilizando o livre consentimento, uma vez que o usuário passa a negar ou aceitar a utilização da ferramenta sem compreender do que se tratava[138].

B) O Interesse Legítimo no RGPD

Assim como a Diretiva 95/46/CE, o RGPD também prevê outras formas legítimas de tratamento de dados que não apenas o consentimento. Essas formas estão dispostas no artigo 6º, nº 1:

> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.
> O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.
> 2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.o 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras

[138] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 179.

> medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX.
> 3. O fundamento jurídico para o tratamento referido no n.o 1, alíneas c) e e), é definido: a) Pelo direito da União; ou b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito.
>
> (...)

A mudança fundamental para trazer previsibilidade e segurança jurídica na aplicação da alínea *f* e evitar que o "interesse legítimo" fosse usado de maneira abusiva para contornar os princípios e regras gerais para tratamento de dados, foi a definição de critérios para o conceito esse conceito jurídico. O Regulamento internalizou a opinião do Grupo do Artigo 29º nos considerandos nº 47 a 50, exigindo que a aplicação dos interesses legítimos levasse em conta as expectativas razoáveis dos titulares dos dados, não podendo prevalecer os seus interesses ou liberdades individuais[139]. Nesse sentido:

> (47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.

Caso o tratamento dos dados seja baseado em um interesse legítimo, ele só poderá ser autorizado se for compatível com as finalidades para as quais os dados tenham sido inicialmente recolhidos. Para confirmar essa compatibilidade, o responsável pelo tratamento necessita verificar a existência de uma ligação entre a primeira finalidade e a finalidade pautada pelo interesse legítimo. Assim está disposto no considerando nº 50:

> (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado

[139] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 250.

> se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior deverá ser considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, deverão ser consideradas tratamento lícito compatível. O fundamento jurídico previsto no direito da União ou dos Estados-Membros para o tratamento dos dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior. A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

Portanto, os critérios para a aplicação dos interesses legítimos devem assegurar a previsibilidade e compatibilidade com os interesses do titular dos dados pessoais. Cabe notar, ainda, que a aplicação da ferramenta de *cookies* sempre dependerá do consentimento prévio do usuário, conforme exige o artigo 5º, nº 3, da Diretiva 2002/58/CE. Entretanto, o tratamento dos dados já coletados por essa ferramenta poderá ocorrer com uma finalidade diversa daquela informada para a aplicação do *cookie*, desde que sejam respeitadas as determinações do Regulamento Geral de Dados Pessoais.

C) Responsabilidade pelo Tratamento de Dados

Os conceitos de responsável pelo tratamento de dados e subcontratante encontrados no artigo 4º do Regulamento seguem as mesmas propostas que a Diretiva 95/46/CE. Assim está disposto:

> Artigo 4.o Definições Para efeitos do presente regulamento, entende-se por:
> 7) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;
> 8) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

Para a aplicação desse conceito, deve ser examinado o contexto fático de cada atividade de tratamento e não o instrumento particular celebrado entre eventual responsável e subcontratante. O responsável pelo tratamento será aquele que toma as decisões acerca do modo e motivo do tratamento de dado, não sendo necessariamente o mesmo agente que coleta os dados. Para a possibilidade de identificação do responsável pelo tratamento de determinados dados que envolva mais de uma empresa, basta responder a seguinte pergunta: A empresa teria realizado a atividade de tratamento de dados da mesma maneira e com o mesmo fim sem a solicitação de uma empresa contratante? Caso a resposta seja positiva, ambas as empresas seriam responsáveis pelo tratamento, pois teriam tomado a decisão. Se a resposta for negativa, a empresa contratante seria a responsável pelo tratamento, enquanto a contratada seria a "subcontratante"[140].

O responsável pelo tratamento tem o papel fundamental de garantir os direitos dos titulares e deve seguir as seguintes obrigações: (i) licitude, lealdade e transparência do tratamento de dados (art. 5º); (ii) registrar as atividades de tratamento (art. 31) e realizar o relatório de impacto sobre proteção de dados (artgs. 35 e 36); (iii) notificar as autoridades de controle e os titulares acerca de qualquer violação de dados ocorrida (artgs. 33 e 34); (iv) cooperar com as autoridades de controle (art. 31); e (v) observar as regras de transferência internacional de dados (artgs. 44 a 50)[141].

Os subcontratantes também possuem obrigações expressas na RGPD, como: (i) garantir a execução de medidas adequadas e organizadas que satisfaçam os requisitos do Regulamento e garantem os direitos dos titulares (art. 28); (ii) vinculação a um contrato com o responsável pelo tratamento com o conteúdo previsto pela RGPD (art. 28); e (iii) registro das atividades de tratamento (art. 30), além das últimas obrigações aplicáveis pelo responsável (notificar acerca de qualquer violação ou vazamento de dados, cooperar com as autoridades de controle e observar as regras de transferência internacional de dados)[142].

Dessa forma, seguindo essa lógica, os sites que abrigam os cookies de terceiros, mesmo que não sejam originalmente subcontratantes, devem ser corresponsáveis pelo tratamento de

[140] MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo, Thomson Reuters, 2018, p. 115.
[141] Ibidem, p. 115.
[142] MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo, Thomson Reuters, 2018, p. 116.

dados na medida da sua participação, concretizando o mencionado entendimento do Grupo do Artigo 29.

D) Direito à Oposição

O usuário tem o direito de se opor ou limitar o tratamento dos seus dados pessoais. Assim define o artigo 21 do Regulamento:

> Artigo 21.o Direito de oposição
> 1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.o 1, alínea e) ou f), ou no artigo 6.o, n.o 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
> 2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
> 3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.
> 4. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.os 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.
> 5. No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.
> 6. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

Ao receber a solicitação de oposição, o responsável pelo tratamento dos dados deve levar em consideração os aspectos pelos quais o processo de tratamento está sendo realizado para consentir ou não o pedido. Conforme o item nº 1 do artigo, o responsável poderá negar o pedido de oposição caso consiga demonstrar que existe legítimo interesse para o processamento ou que seja necessário por razões legais.

O dispositivo ainda permite um controle do usuário na definição do seu perfil e na comercialização direta de dados com terceiros. Em relação a criação de perfil por decisões totalmente automatizadas, o usuário possui o direito de pelo menos obter a intervenção de uma pessoa natural por parte do responsável para que possa manifestar seu ponto e contestar a decisão (art. 22).

Dessa forma, o consentimento poderia ser feito de maneira fragmentada, aumentando a liberdade do cidadão em definir as condições do tratamento de seus dados. Entretanto, o exercício da oposição se concretiza após o consentimento. Ou seja, o usuário consente com tudo e depois pode se opor. Na utilização de *cookies* isso é ainda mais difícil de ocorrer, uma vez que as empresas apresentam muitas vezes todos os *cookies* em conjunto, exigindo uma capacidade técnica superior a de um cidadão comum para distingui-los.

Ante o exposto, pode-se concluir que apesar de haver outras formas de legitimar o tratamento de dados pessoais, a mais relevante no contexto da RGPD é por meio do consentimento. Quando se trata especificamente do uso da ferramenta de *cookies*, o consentimento está inteiramente presente, devendo ser prévio, livre, inequívoco, informado e explícito. Não obstante a incontroversa importância do consentimento para garantir a autodeterminação informativa do cidadão em relação ao uso de seus dados, esse método por si só possui fragilidades e muitas vezes as suas adjetivações não são garantidas em sua totalidade.

Dessa forma, como será visto no capítulo quatro do presente trabalho, não apenas a fragmentação do consentimento é fundamental para que o cidadão seja realmente livre em suas escolhas sobre o uso de dados pessoais sem sofrer represálias, sobretudo no que diz respeito à utilização de *cookies* pelo mercado digital. Para a verdadeira eficácia da legislação, deve haver outros meios de regulação para a proteção de dados pessoais.

CAPÍTULO 3: PROTEÇÃO DE DADOS E REGULAÇÃO DO USO DE *COOKIES* NO BRASIL

Atualmente, não há nenhuma lei unitária de proteção de dados em vigor no Brasil e nem uma regulação direta sobre o uso de *cookies*, como a Diretiva 2002/58/CE no ordenamento comunitário europeu. Entretanto, podem ser encontrados diversos mecanismos constitucionais e infraconstitucionais que fundamentam, mesmo que de maneira incompleta, a proteção de dados pessoais[143].

Como já foi explanado no primeiro capítulo, subitem 1.1.2, como a proteção de dados pessoais ainda não é prevista na Constituição Federal como um direito fundamental, o

[143] MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018, p. 167.

ordenamento jurídico brasileiro necessita reinterpretar as garantias constitucionais para enquadrá-lo na tutela constitucional. Cabe lembrar que o Brasil adotou o sistema de reconhecimento de direitos fundamentais aberto[144], ou seja, os direitos previstos no artigo 5º da Constituição Federal não é um rol taxativo.

Nesse sentido, ao interpretar a ação intitulada de *habeas data*, introduzida no art. 5º, inciso LXXII, da Constituição Federal, que reconhece a proteção constitucional das informações pessoais, juntamente ao princípio da dignidade humana, cria espaço para a ampliação dos direitos à proteção da privacidade e intimidade e do sigilo de informação e comunicação, à proteção de dados pessoais[145].

Pretendendo criar um reconhecimento expresso da proteção de dados pessoais como um direito fundamental autônomo, a Comissão de Constituição, Justiça e Cidadania (CCJ) aprovou, no dia 22/05/2019, a PEC 17/2019[146], que pretende acrescentar os incisos XII-A, ao artigo 5º, e XXX, ao artigo 22, assim dispostos:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> XII - A - é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais.
>
> Art. 22. Compete privativamente à União legislar sobre:
> (...)
> XXX- proteção e tratamento de dados pessoais;

Um dos principais motivos para a emenda é a preocupação como o surgimento de diversas legislações estaduais e municipais próprias, que podem trazer conceitos próprios, muitos deles inconstitucionais, e dificultar a tutela desse direito de maneira uniforme. Assim dispõe o texto da Emenda Constitucional[147]:

> Sabemos que existem diversas propostas de leis estaduais e municipais versando sobre o assunto, inclusive em flagrante réplica da LGPD. Não há racionalização nisso: a fragmentação e pulverização de assunto tão caro à sociedade deve ser evitada. O ideal, tanto quanto se dá com outros direitos fundamentais e temas gerais relevantes, é que a União detenha a competência central legislativa. Do contrário, pode -se correr o

[144] BRASIL, Constituição da República Federativa de 1988, artigo 5º, §2º: "§ 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte." Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso dia: 26/05/2019.
[145] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 172.
[146] BRASIL, PEC 17/2019.
[147] BRASIL, PEC 17/2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1560427715849&disposition=inline

> risco de, inclusive de forma inconstitucional, haver dezenas - talvez milhares- de conceitos legais sobre o que é "dado pessoal" ou sobre quem são os "agentes de tratamento" sujeitos à norma legal. Impõe-se, portanto, que o país apresente uma legislação uniforme quanto à proteção e tratamento de dados, tendo em vista ser praticamente impossível aos governos e empresas de todo o mundo se adaptarem a normas específicas de cada localidade. Além disso, a pluralidade normativa pode trazer problemas de compatibilidade e adequação dos dados, em especial nos serviços disponibilizados pela rede mundial de computadores, que utilizam os dados pessoais de formas cada vez mais abrangentes e inovadoras.

Em 2018, foi publicada a Lei nº 13.709/18, inspirada pelo RGPD, chamada de lei Geral de Proteção de Dados (LGPD). Essa lei regula de maneira específica a questão da proteção de dados no país, pretendendo preencher as lacunas e complementar as demais leis que, de uma forma ou de outra, regulamentam o uso de dados no país. Entretanto, ela essa lei entrará em vigor apenas em 2020, dando um espaço de dois anos para que as instituições possam se organizar de acordo com a nova lei. Portanto, atualmente o Brasil depende de outros diplomas legais para tutelar esse tema.

Dentre as diversas leis contribuem para a tutela da proteção de dados pessoais no país, algumas serão expostas a seguir para que se possa verificar quais os princípios que nortearam o país até a criação da LGPD.

3.1 – Leis Setoriais sobre Proteção de Dados

3.1.1 O Código de Defesa do Consumidor (Lei nº 8.078/90)

O Código de Defesa do Consumidor foi a primeira lei que tratou de forma moderna a proteção da privacidade e aos dados pessoais, tendo em vista as novas tecnologias criadas[148]. Em seu artigo 43, o código disciplinou a questão dos bancos de dados e dos cadastros dos consumidores, dispondo da seguinte maneira[149]:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

[148] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 141.
[149] BRASIL, Lei nº 8.8078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso dia 10/06/2019.

> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

O diploma em questão alcança todo e qualquer dado pessoal do consumidor, atingindo qualquer banco de dados que interfira no livre desenvolvimento da personalidade do consumidor[150]. Nota-se que o Código de Defesa do Consumidor buscou conferir a autodeterminação informacional dos consumidores ao abarcar princípios que norteiam a proteção de dados pessoais na maior parte dos países, inclusive a União Europeia.

Em uma análise do disposto no artigo 43, depreende-se a possibilidade do acesso do cidadão sobre todas as informações que digam respeito a ele e da correção imediata de qualquer dado errado ou inexato. Além disso, os consumidores devem ser avisados da abertura do cadastro ou registro de dados pessoais de consumo, que devem conter informações objetivas, claras, exatas e em linguagem de fácil compreensão (princípio da transparência) e do limite temporal para o armazenamento dos dados (princípio do esquecimento)[151]. É interessante notar que esses são alguns dos direitos e princípios basilares da RGPD (e da LGPD).

3.1.2 Código Civil (Lei nº 10.406/2002)

O Código Civil possui um capítulo exclusivo para a tutela do direito à personalidade. Sobre o direito à privacidade está assim disposto:

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.[152]

[150] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 127.
[151] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 143.
[152] BRASIL, Lei nº 10.406, de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso dia 11/06/2019.

Apesar da disposição vaga e genérica na previsão acerca do direito à privacidade, ao ser interpretado em conjunto coma as demais normas de privacidade o artigo 21 adquire uma maior importância. Isso porque além de concretizar o direito fundamental no direito civil, a norma deixa claro a natureza jurídica do bem protegido, evidenciando a tutela da privacidade como inerente à dignidade humana e à personalidade do indivíduo[153].

Ademais, ao ser aplicado subsidiariamente ao Código de Defesa do Consumidor, essa norma consolida o conceito de direito à privacidade do consumidor. Por outro lado, ao prever eventual obrigação de fazer ou não fazer definida por juiz que, a requerimento do interessado, note uma violação na sua vida privada, o Código Civil estabelece outro mecanismo de proteção ao lado da responsabilidade civil[154].

3.1.3 Lei do Cadastro Positivo (Lei nº 12.414/2011)

A Lei do cadastro Positivo também foi responsável por estabelecer princípios do direito a proteção de dados no ordenamento brasileiro. Ela disciplina a criação e a consulta de bancos de dados com informações de adimplemento para a criação de histórico de crédito, ampliando o fluxo de dados no mercado. Em contrapartida essa lei também criou limitações para a coleta de dado e mecanismos de controle para a proteção à privacidade, determinando, por exemplo, que as informações sejam objetivas, claras, verdadeiras e de fácil compreensão. Mesmo que essas limitações se apliquem ao contexto específico de histórico de créditos, essa disposição foi relevante para o futuro da regulação geral de proteção de dados.

Primeiramente, cabe evidenciar que a lei exige o consentimento do titular dos dados pessoais, que deve ser externado por meio de assinatura, em instrumento específico ou em cláusula apartada[155], além de exigir a expressa autorização do titular para compartilhamento de suas informações (art. 9). Nesse sentido, é relevante observar que a lei permite um controle maior do cidadão sobre o destino dos seus dados.

---

[153] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 144.

[154] Ibidem, p. 145.

[155] Art. 4º A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada.
§ 1º Após a abertura do cadastro, a anotação de informação em banco de dados independe de autorização e de comunicação ao cadastrado.
§ 2º Atendido o disposto no caput, as fontes ficam autorizadas, nas condições estabelecidas nesta Lei, a fornecer aos bancos de dados as informações necessárias à formação do histórico das pessoas cadastradas.

O artigo 5º do diploma legal, tece outras relevantes determinações para a proteção de dados pessoais, conforme as suas disposições:

> Art. 5º São direitos do cadastrado:
> I - obter o cancelamento do cadastro quando solicitado;
> II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar as informações de adimplemento;
> III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele compartilhou a informação;
> IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
> V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento;
> VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
> VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

Nota-se, com isso, a presença dos seguintes direitos: (i) direito de esquecimento (inciso I); (ii) direito do acesso às informações pelo titular dos dados (inciso II); direito de retificação ou cancelamento de informações erradas ou inexatas (inciso III); direito de adquirir os dados do responsável pelo banco de dados (inciso V); uso dos dados para a única e exclusiva finalidade para que foram coletados de acordo com o consentimento do titular (incisos V e VII); e o inovador direito à revisão das decisões realizadas por meios exclusivamente automatizados (inciso VI).

A lei reconhece, ainda, a existência de dados sensíveis, como informações sobre origem social e étnica, orientação sexual, estado de saúde, convicções políticas e outras que podem acarretar na discriminação do consumidor[156]. Assim dispõe o artigo 3º, § 3º:

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
> § 3º Ficam proibidas as anotações de:
> I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e
> II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

[156] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 146.

Essas limitações permitem uma maior emancipação do consumidor no controle de suas próprias informações pessoais, consolidando a evolução do conceito de autodeterminação informativa no ordenamento brasileiro[157].

3.1.4 Marco Civil da Internet (Lei nº 12.965/2014)

O Marco Civil da Internet inaugurou regras específicas que contribuem para a proteção da privacidade na rede mundial de computadores, apresentando princípios e garantias, direitos e deveres para o uso da Internet no país. Um dos pilares da lei é a proteção dos dados pessoais dos usuários e a liberdade de expressão, conforme prevê o artigo 3º[158]:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> (...)
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

O Marco Civil da Internet teve como inspiração os artigos 7 e 8 da Carta de Direitos Fundamentais da União Europeia, e inova ao reconhecer a proteção à privacidade e ao dados pessoais como direitos distintos, "o que significa dizer que nem sempre que houver violação a dados pessoais haverá violação ao direito da privacidade, e vice-versa, entendimento que fortalece a aplicação da proteção de dados pessoais"[159].

Nesse sentido, o artigo 7º da lei introduz princípios e obrigações relevantes para a proteção de dados pessoais na internet:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

---

[157] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 147.

[158] BRASIL, Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso dia 13/06/2019.

[159] SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina. Marco Civil da Internet: Jurisprudência Comentada. 2ª tiragem. São Paulo: Revista dos Tribunais, 2018, p. 20.

> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Trata-se do dispositivo mais importante para a tutela da proteção de dados pessoais, sendo o Marco Civil da Internet a lei em vigência mais importante sobre o tema no país (enquanto a LGPD não produz efeitos). A lei faz menção à necessidade do consentimento do usuário para a coleta, uso, armazenamento, compartilhamento e tratamento de dados pessoais, adjetivando o consentimento como devendo ser livre, expresso e informado. O responsável pelo tratamento deve, ainda, prestar informações claras e completas, utilizando-se de cláusulas contratuais destacadas e dando publicidade às políticas de uso[160]. De modo a concretizar a autodeterminação informativa do cidadão, a lei em comento ainda prevê a possibilidade de exclusão definitiva dos dados fornecidos para determinada aplicação (artigo 7º, inciso X).

Apesar de não haver uma regulação específica do uso da ferramenta de *cookies* no Brasil, o Marco Civil da Internet determina obrigações que interferem no uso dessas ferramentas pelos *sites* que atuam no território nacional. Segundo o inciso VIII, do seu artigo 7º, a legislação exige que o responsável justifique a finalidade da coleta e tratamento dos dados pessoais, devendo haver um termo de uso com informações claras e completas acerca do tratamento. Por meio desse termo de uso o usuário deve aceitar a coleta e tratamento de dados.

[160] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 132.

Assim, caso sejam utilizados *cookies* para a coleta de dados, o responsável deve informar os usuários acerca dessa ferramenta, que pode ser ou não aceita.

Além disso, o artigo 7º, inciso VII da lei, estabelece condições para a transferência de dados pessoais pelas empresas, o que vincula diretamente o uso de *cookies* de terceiros pelos *websites*. Conforme o dispositivo, o fornecimento a terceiros de registros de conexão e acesso a aplicações da internet só podem ser transferidos mediante consentimento livre, expresso (inciso IX) e informado (ou em hipóteses previstas em lei) pelo titular dos dados pessoais. Dessa forma, todo uso de *cookies* de terceiros deve ser informado aos usuários e só pode funcionar com a sua autorização expressa.

Nesse sentido, a autora Laura Schertel Mendes afirma[161] que:

> Para passar pelo pressuposto objetivo de legitimidade, os cookies, em nenhum dos casos, podem apresentar graves riscos para os usuários. Isto é, em nenhuma hipótese é legítimo submeter o usuário a uma vigilância ininterrupta, transformando-o em mero objeto de monitoramento, o que, naturalmente, violaria o seu direito à intimidade e à vida privada e o princípio da dignidade, protegidos constitucionalmente. Além disso, em qualquer dos casos é preciso que seja divulgada por meio da política de privacidade ou no contrato de prestação de serviços da empresa publicado no site a forma de utilização dos cookies e para quais finalidades eles são instalados (7.°, VI, VIII e XI, Marco Civil, e art. 6.°, III do CDC).

Contudo, a regulação do uso de *cookies* pelo Marco Civil da Internet ainda é nebulosa. Dependendo da interpretação da norma, o exercício do consentimento poderia ser exercido como um direito de recusa posteriormente ao acesso. Além disso, caso o usuário não se pronuncie acerca do uso, poderia ser considerado como um consentimento tácito, ou o adjetivo expresso exige a ação de clicar em alguma opção? Essa falta de especificidade da lei permite que a maioria dos *sites* em funcionamento no país ainda utilize a ferramenta de *cookies* sem nenhum aviso claro ao consumidor, levando em consideração que não é um costume o indivíduo abrir todos os termos de uso dos sítios eletrônicos que visita.

Ademais, não há nenhuma previsão na lei que impeça a empresa de impedir o acesso caso aos serviços caso o usuário não aceite o uso da ferramenta de *cookie*, inviabilizando o consentimento livre do cidadão que fica entre a dualidade de "pegar ou largar". Dessa forma, não obstante os avanços significativos e revolucionários no ordenamento brasileiro, trazidos pelo Marco Civil da Internet para a proteção de dados pessoais, ainda faltam disposições

[161] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014, p. 225.

eficazes que clarifiquem a regulação do uso de testemunhos de conexão para a concretude da autodeterminação informacional dos cidadãos.

A ausência de legislação específica causa interpretações abstratas de alguns conceitos essenciais sem um significado prático e que possa ter aplicabilidade imediata.

3.2 – Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)

O Marco Civil da Internet proporcionou primeiros passos para a redação de uma lei específica de proteção de dados pessoais. Após quase uma década, foi finalmente aprovada a Lei Geral de Proteção de Dados Pessoais no Brasil, que trata da proteção de dados em qualquer relação que envolva tratamento, seja por instituições públicas ou privadas; seja por pessoa natural ou jurídica. Essa nova lei, que entrará em vigor no ano de 2020, dispõe de princípios, direitos e obrigações para o uso de dados e reúne diversos mecanismos de controle para assegurar o cumprimento das garantias de proteção dos direitos humanos[162].

Cumpre salientar que o regime de proteção de dados não possui apenas o objetivo de tutelar a privacidade dos usuários[163], mas "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade de pessoa natural", além do desenvolvimento tecnológico e econômico do país, conforme consta no seu artigo 1º. Além disso, a norma está baseada nos seguintes fundamentos[164]:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Assim como na RGPD, a lei brasileira apresenta, em seu artigo 5º, conceitos-chave para a sua aplicação. Dado pessoal é definido como toda informação relacionada a pessoa natural

[162] PINHEIRO, Patricia Peck. Proteção de Dados Pessoas: Comentários à Lei nº 13.709/2018 (LGPD). 1ª ed. São Paulo: Saraiva, 2018, p. 15.
[163] FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-08-30-A nova Lei Geral de Protecao de Dados Pessoais Principais repercussoes para a atividade empresarial Parte_I.pdf. Acesso dia 15/06/2019.
[164] BRASIL. Lei nº 13.709, de 14 de agosto de 2018.

identificada ou identificável (art. 5º, inciso I), e dado sensível como o 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, quando vinculado a uma pessoa natural" (art. 5º, II). Com isso, é possível perceber que o campo de aplicação da norma é extremamente amplo. Nota-se, também, que a lei não considera como passível de proteção os dados de uma pessoa jurídica, mas apenas pessoa natural (art. 5º, V).

Apesar da previsão legal de que pessoa jurídica não pode ser titular de dados pessoais, o mesmo não se pode falar do controlador (responsável pelo tratamento de dados) e do operador (subcontratado). Como se extrai do artigo 5º, inciso VI, o controlador é toda "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", enquanto operador é toda "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

A LGPD não se aplica, contudo, ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, jornalísticos, artísticos ou acadêmico, ou, ainda, para fins de segurança pública, defesa nacional, segurança do Estados e atividades de investigação e repressão de infrações penais, que deverão ser tratados por meio de lei própria (artigo 4º). Além disso, os dados anônimos também não são objeto de aplicação da lei, salvo quando o processo de anonimização puder ser revertido (art. 12).

Segundo a norma, tratamento de dados é toda a operação realizada com dados pessoais, como (mas não somente) a coleta, produção, recepção, transmissão, acesso, distribuição, armazenamento, transferência e processamento (art. 5º, X). Nas palavras da autora Ana de Oliveira Frazão[165]:

> Como se pode observar, o conceito de tratamento de dados é extremamente amplo, o que ajuda a entender que a lei, tal como previsto no seu art. 3º, aplica-se a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada em território nacional ou em casos em que os dados pessoais forem coletados no Brasil, digam respeito a indivíduos localizados em território nacional ou o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços no Brasil.

[165] FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I.

Seguindo o mesmo entendimento da legislação comunitária europeia e do Marco Civil da Internet, artigo 6º da lei[166] expõe os princípios que orientam a proteção proporcionada pela LGPD, sendo os princípios da: finalidade (inciso I); adequação (inciso II); necessidade (inciso III); livre acesso (inciso IV); qualidade dos dados (inciso V); transparência (inciso VI); segurança (inciso VII); prevenção (inciso VIII); não discriminação (inciso IX); e responsabilização e prestação de contas (inciso X). Esses pilares principiológicos são fundamentais para a interpretação dos dispositivos da lei.

Apesar de não se manifestar expressamente acerca do uso da ferramenta de *cookies*, os conceitos e princípios apresentados pela Lei Geral de Proteção de Dados Pessoais demonstram que há uma incidência direta da aplicação da norma no uso dessa ferramenta pelas empresas. De acordo com o que será apresentado a seguir, será possível concluir que mesmo sem nenhuma norma específica sobre os testemunhos de conexão, o Brasil poderá regular o seu uso de forma semelhante à União Europeia quando a LGPD.

Entretanto, apesar das questões positivas trazidas pelas semelhanças, o ordenamento brasileiro também interioriza os problemas já enfrentados nos países que integram a comunidade europeia sem, contudo, apresentar uma proposta alternativa.

---

[166] Nesse sentido:
"Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: 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;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

3.2.1 O Consentimento na LGPD

O artigo 5º, inciso XII, define consentimento da seguinte maneira:

> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

A aplicação do consentimento para o tratamento de dados legítimos está prevista nos artigos 7º e 8º, que dispõem:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
> (...)

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

O consentimento é, portanto, altamente qualificado, devendo a manifestação de vontade ser livre, inequívoca, informada e específica. Dessa forma, as informações dadas pelo responsável pelo tratamento de dados devem ser claras, específicas e com a finalidade explícita, caso contrário, o consentimento genérico para o tratamento de dados será considerada nulo[167]. O artigo 8º ainda prevê que o consentimento deve ser dado por meio escrito "ou por outro meio

[167] FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – A Importância do Consentimento para o Tratamento dos Dados Pessoais, Parte III. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-09-12-A_nova_Lei_Geral_de_Protecao_de_Dados_Repercussoes_para_a_atividade_empresarial_a_importancia_do_consentimento_para_o_tratamento_dos_dados_pessoais_Parte_III.pdf. Acesso dia 15/06/2019.

que demonstre a manifestação de vontade do titular", devendo o ônus da prova recair sobre o controlador.

Interpretando esse dispositivo conforme os objetivos e princípios da lei, o consentimento de forma escrita para cada *cookie* é impensável, uma vez que as empresas não teriam condições de solicitar que cada usuário se pronunciasse por escrito, o que iria inviabilizar o negócio e contrariar o objetivo da própria lei conforme o art. 2º[168]. Entretanto, o consentimento realizado deve ser inequívoco para ser válido, cabendo ao responsável pelo tratamento de dados tomar providências para a sua realização, visto que o consentimento tácito não produz efeitos. Na hipótese me que o tratamento de dados está vinculado à prestação de serviços, o titular deve ser avisado de maneira clara acerca da situação (art. 9º) e sobre os meios que poderá exercer os seus direitos.

Sempre que o controlador necessitar comunicar ou compartilhar os dados com terceiros, deve haver consentimento expresso do titular, ressalvadas as hipóteses de dispensa do consentimento definidas pela lei. Nesse sentido, tanto aquele que compartilhou os dados quanto aquele que os recebeu são solidariamente responsáveis pelo tratamento. Assim afirma Ana de Oliveira Frazão[169]:

> Com isso, cria-se dever que, longe de se restringir ao controlador originário - aquele que coletou ou tratou originariamente os dados -, estende-se a todos aqueles que irão ter acesso aos dados, dos quais se exige o dever de verificar a licitude do procedimento de acesso ou compartilhamento, inclusive no que diz respeito ao consentimento específico do titular

Assim, é possível a interpretação de que a LGPD seguiu o entendimento do Grupo do Artigo 29º de que tanto o provedor que permitiu a aplicação dos *cookies* de terceiros quanto o próprio proprietário da ferramenta são responsáveis pelo tratamento dos dados pessoais realizados por ela.

3.2.2 Interesse Legítimo

Além do consentimento, a Lei Geral de Proteção de Dados Pessoais prevê outras formas de tratamento legítimo de dados sem a necessidade de autorização do titular. A mais relevante

[168] BRASIL. Lei nº 13.709, de 14 de agosto de 2018, artigo 2º, inciso V: "o desenvolvimento econômico e tecnológico e a inovação".

[169] FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – A Importância do Consentimento para o Tratamento dos Dados Pessoais, Parte III.

para a análise da regulação do uso da ferramenta de *cookies* é a hipótese presente no artigo 7º, inciso IX, que determina o seguinte:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> IX - 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;

Sobre o legítimo interesse a lei afirma:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

O conceito vago e ambíguo de interesse legítimo gera uma dificuldade na doutrina para tentar enquadrar os seus limites na proteção dos dados pessoais dos cidadãos. A amplitude do conceito pode mitigar por completo a principal regra para o tratamento de dados, ou seja, o consentimento[170]. De modo a tentar amenizar os problemas provenientes da abstração do conceito de legítimo interesse, deve-se interpretar o dispositivo em conjunto com o princípio da finalidade, limitando o legitimo interesse não apenas à necessidade do controlador, como também por meio de uma avaliação dos impactos sobre os direitos dos titulares dos dados[171].

Diferentemente da RGPD, o legítimo interesse do controlador como justificativa para a licitude do tratamento de dados pessoais pode banalizar o uso de *cookies* pelos *sites*. Assim como ocorria na União Europeia com a diretiva 95/46/CE, o conceito abstrato dessa hipótese torna os direitos e garantias fundamentais dos cidadãos vulneráveis e fragiliza a autodeterminação informativa no Brasil.

---

[170] FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – As Demais Hipóteses para o Tratamento dos Dados Pessoais, Parte IV. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-09-20-A nova Lei Geral de Protecao de Dados Repercussoes para a atividade empresarial as demais hipoteses de tratamento de dados pessoais Parte IV.pdf. Acesso dia: 15/06/2019.

[171] Ibidem.

3.2.3 Direito à Oposição

A transparência das informações na proteção de dados pessoais é um dos princípios que regem a LGPD. Para a sua adequada exteriorização, o titular deve ter fácil acesso a informações claras acerca da finalidade, forma e duração do tratamento, além das informações relativas aos agentes que realizam o tratamento. Essa garantia é fundamental para que o cidadão possa exercer o seu direito à oposição. Nesse sentido:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.
> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
> § 2º 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.
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Assim como no Regulamento da União Europeia, a LGPD também prevê a possibilidade do titular de se opor ou limitar o tratamento de seus dados pessoais. Esse direito reafirma o controle do usuário sobre os seus dados e confirma a sua autodeterminação informacional, principalmente quando decisões automatizadas criam perfis que afetam a vida privada do indivíduo. Dessa forma, o artigo 20 da lei nacional de proteção de dados pessoais dispõe o seguinte:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional

> poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Assim, em face da nova economia pautada pelo uso de dados pessoais e a evolução tecnológica que cria mecanismos cada vez mais sofisticados para o tratamento cada vez mais rápido de dados, a LGPD garante um devido processo legal para proteger os cidadãos dos julgamentos das decisões automatizadas, criando um bloco de direitos que permitem (i) o acesso a informações que dizem respeito aos procedimentos utilizados pelas decisões automatizadas; (ii) a oposição das dessas decisões, permitindo o titular manifestar o seu ponto de vista; (iii) a revisão das decisões por uma pessoa natural; e (iv) recurso à autoridade nacional para a realização de auditoria quando as informações não forem prestadas[172].

CAPÍTULO 4: ANÁLISE DA REGULAÇÃO DO USO DE *COOKIES* E A POTENCIAL EFICÁCIA DAS LEGISLAÇÕES

Ante todo o exposto, é notável as semelhanças entre a regulação europeia e a brasileira acerca da proteção de dados pessoais. Apesar de disporem de diferentes hipóteses para um tratamento de dados legítimos, o consentimento ainda é o pilar de ambas. Entretanto, em um plano geral, essas legislações também apresentam falhas que dificultam a aplicação dos seus objetivos no mercado.

Tendo isso em vista, partiremos para a parte final desse estudo, na qual serão analisados os principais problemas para a devida aplicação das normas e quais as soluções possíveis para contornar esse problema.

4.1 – Semelhanças e Diferenças entre as Regulações Europeia e Brasileira

O modelo brasileiro de proteção de dados pessoais adota, em sua maior parte, inspiração nos modelos consolidados da União Europeia. Por essa razão, existem grandes similitudes entre

[172] FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – O Direito à Oposição e à Explicação Diante de Decisões Totalmente Automatizadas, Parte XV. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-12-06-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_o_direito_a_explicacao_e_a_oposicao_diante_de_decisoes_totalmente_automatizadas_Parte_XV.pdf. Acesso dia 15/06/2019.

as duas legislações, sobretudo na hipótese do consentimento como base legal principal[173] para a licitude do tratamento de dados pessoais dos cidadãos.

Em uma análise comparada entre os dois modelos, observa-se que o consentimento possui grande adjetivação em ambas as legislações, devendo ser livre, inequívoco, expresso, específico e informado. Para que isso seja possível, o responsável pelo tratamento de dados deve seguir diversos princípios que regem esse tema. Como destaque, o princípio da transparência exige que sejam dadas informações claras, de fácil compreensão e específicas com a finalidade do uso dos dados.

As informações são fundamentais para o exercício irrestrito do direito à escolha do titular, consolidando o consentimento livre. Dessa forma, qualquer mudança de finalidade do tratamento de dados deve ter a anuência do titular. Além disso, há um dever do responsável em informar as consequências da negativa do consentimento[174], como por exemplo, a impossibilidade do funcionamento de algum serviço que dependa de tratamento de dados. O descumprimento desses requisitos torna nulo o consentimento do titular e acarreta a responsabilização do controlador. Isso confirma a importância da autodeterminação informacional do cidadão.

Há também, a exigência do oferecimento dos dados do responsável pelo tratamento para que o titular tenha conhecimento de quem está utilizando os seus dados (o responsável não pode ser anônimo) e amparo sobre qualquer tipo de problema, uma vez que o tratamento desconforme com o que foi consentido deve gerar reparação por parte do responsável. Além disso, a vontade do titular deve ser continuada, ou seja, o consentimento pode ser retirado a qualquer momento e deve ser tão fácil quanto dar.

Ambas as legislações determinam o direito à oposição do tratamento de dados pelos titulares, tanto daqueles permitidos pelo interesse legítimo do responsável quanto daqueles realizados por decisões automatizadas. Contudo, há diferenças nas normas que merecem

[173] Nesse sentido: "Por outro lado, também é possível dizer que o consentimento não deixou de ser o seu vetor principal (como base legal para tratamento de dados). Isso porque uma análise detida dos princípios e a maneira pela qual a LGPD disseca tal elemento ao longo do seu corpo normativo acabam por revelar uma forte preocupação, mais uma vez, sobre qual deve ser a carga participativa do indivíduo no fluxo de suas informações pessoais. Primeiro, por adjetivar extensamente o consentimento seguindo a linha evolutiva do direito comunitário europeu (...). Segundo, porque a grande parte dos seus princípios tem todo o seu centro gravitacional no indivíduo." BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 134.

[174] Na LGPD, por exemplo, essa necessidade está prevista no artigo 18, inciso VIII.

atenção. No artigo que prevê o direito à oposição na RGPD está disposto o seguinte (grifou-se):

> Artigo 21.o Direito de oposição
> 1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.o 1, alínea e) ou f), ou no artigo 6.o, n.o 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
> 2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
> 3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim. 4.5.2016 PT Jornal Oficial da União Europeia L 119/45
> 4. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.os 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.
> 5. No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.
> 6. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.o, n.o 1, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o tratamento for necessário para a prossecução de atribuições de interesse público.

> Artigo 22.o Decisões individuais automatizadas, incluindo definição de perfis
> 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
> 2. O n.o 1 não se aplica se a decisão:
> a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;
> b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou
> c) For baseada no consentimento explícito do titular dos dados.
> 3. Nos casos a que se referem o n.o 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.
> 4. As decisões a que se refere o n.o 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.o 1, a não ser que o n.o 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

Já na LGPD está disposto na seguinte forma (grifou-se):

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Como se pode depreender dos textos normativos, o tratamento de dados baseado no interesse legítimo do responsável pode ser contestado pelo titular dos dados pessoais. No direito europeu, o responsável deve cessar o tratamento "a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial". Note-se que há uma proteção maior à autodeterminação informacional do titular no âmbito europeu, uma vez que (i) incumbe-se ao responsável a comprovação de que o seu interesse legítimo prevalece sobre os direitos, interesses e liberdades do titular; e (ii) a contestação do titular não está limitada a uma ação ilegal do responsável, sendo qualquer uma que não prevaleça sobre seus direitos.

Por outro lado, no contexto brasileiro, existe uma maior dificuldade para o titular contestar o tratamento de dados baseados nos interesses legítimos do responsável, tendo em vista (i) que só poderá contestar o tratamento realizado em descumprimento com a LGPD; e (ii)

o conceito vago e ambíguo de interesse legítimo, que gera uma dificuldade de limitação no contexto da proteção de dados, podendo mitigar a principal regra para o tratamento de dados, ou seja, o consentimento.

Como já observado, o direito comunitário europeu passou por problemas causados pela falta de definição concreta do que poderia ser considerado interesse legítimo durante a vigência da Diretiva 95/46/CE, levando o Parlamento Europeu delimitá-lo nos considerandos 47 a 50 do Regulamento Geral de Proteção de Dados.

Na esfera do uso da ferramenta de *cookies,* essa indefinição pode acarretar desafios maiores para a limitação do uso abusivo dessa ferramenta pelas empresas, criando mecanismos que possam contornar os direitos e princípios previstos pela lei. Esse caso ainda pode se agravar, pois, no ordenamento brasileiro, ao contrário da União Europeia que vincula o uso da ferramenta ao consentimento prévio do cidadão por meio da Diretiva 2002/58/CE, não há uma legislação específica sobre o assunto, podendo o uso de *cookies* se basear unicamente no interesse legítimo do responsável.

Por fim, faz-se relevante mencionar que ambas as legislações exigem a transparência acerca da formação de perfis, devendo o responsável pelo tratamento de dados informar o procedimento utilizado para a decisão. Ademais, os titulares de dados pessoais têm o direito de se oporem às decisões automatizadas para manifestarem seu ponto de vista e o direito de obtenção da revisão da decisão automatizada por uma pessoa natural

4.2 – O Desafio do Consentimento na Regulação da Ferramenta de *Cookies*

Conforme já explanado, apesar da existência de outras hipóteses legais de tratamento de dados, o consentimento do titular continua sendo o principal garantidor da autodeterminação informacional do cidadão. Observa-se que ambas as legislações colocam o indivíduo como principal regulador dos seus próprios dados em uma tentativa de proteger seus direitos fundamentais.

Contudo, a crença de que o cidadão é um sujeito racional e que conseguirá desempenhar a sua autodeterminação informacional e realizar um processo racional de tomada de decisões acerca do uso de seus dados pessoais não é necessariamente correta se levarmos em

consideração toda complexidade do fluxo informacional[175]. Os inúmeros atores envolvidos na comercialização de dados pessoais tornam esse ecossistema muito mais complexo, exigindo que o cidadão tenha consciência a respeito de todos eles para que consiga gerenciar as suas informações pessoais[176].

Além da dificuldade de memorizar os inúmeros atores que compõem o campo de comercialização de dados pessoais, o indivíduo ainda precisa compreender como os seus dados pessoais serão tratados por cada um deles, uma vez que todos possuem diferentes políticas de privacidade e tratamento de dados. Essa rede complexa cria barreiras psicológicas no ser humano que inviabilizam a tomada de decisão consciente acerca do uso de seus dados[177].

Uma dessas barreiras que já impõe desafios à uma legislação pautada pelo consentimento como base principal para o tratamento de dados, é a chamada teoria da utilidade subjetiva[178]. O ser humano possui a tendência de focar em benefícios imediatos e, por essa razão, deixa de ponderar possíveis prejuízos que são distantes e, uma vez feita a escolha, dificilmente retirará o seu consentimento[179]. Por essa razão, por mais que a pessoa compreenda o valor dos seus dados pessoais, a dificuldade de se conhecer todos os atores envolvidos e a tendência em valorizar os benefícios imediatos (serviços *online*), acabam contradizendo o que elas enxergam como ideal (proteção de seus dados).

Além disso, a maior parte dos consumidores não possui conhecimento técnico para autodeterminar os seus dados pessoais. Em uma pesquisa realizada pela Universidade de Stanford[180] sobre a coleta de dados pessoais dos usuários por meio da ferramenta de *cookie*, dentre as pessoas entrevistadas 17% afirmaram deletar os *cookies*, 23% não tinham certeza e 60% não deletavam. Ao indagar o motivo pelo qual as pessoas não deletavam essa ferramenta, a maioria das respostas era porque "alguém recomendou que fizesse", sendo apenas um terço aquelas que realmente apagavam por questões relacionadas a privacidade[181].

---

[175] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 148.
[176] Ibidem, p. 146.
[177] Ibidem, p. 147.
[178] KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. *Soft surveillance, hard consent.* In: KERR, Ian (Ed.) *Lessons from identity trail: anonymity, privacy and identity in a networked society.* New York: Oxford University Press, 2009, p. 17 *apud* BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 147.
[179] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 147.
[180] Ibidem, 149.
[181] Ibidem, p. 150.

Dessa forma, percebe-se que a pretensão de um consentimento livre já nasce corrompido, uma vez que a própria falta de conhecimento técnico e a limitação cognitiva afasta os consumidores de uma tomada de decisão livre e consciente. Por essa razão, as legislações europeia e brasileira exigem informações de fácil acesso, claras e em linguagem de fácil compreensão para tentar amenizar esse problema e garantir a autodeterminação informacional dos cidadãos. Entretanto, como efeito disso, os consumidores passaram a ser bombardeados por banners, avisos e informações de políticas de privacidade para que pudessem dar o seu consentimento informado, e acabaram aceitando ou recusando sem compreender o que realmente estava disposto.

Por essa razão, os cidadãos demorariam muito tempo para ler todas as políticas de privacidade para tomar ciência de todas as práticas com os seus dados para depois poder tomar uma decisão consciente sobre aceitá-las ou não. Isso certamente é inviável, motivo pelo qual as normas não são tão eficazes quanto poderiam ser. Para mudar esse cenário, os ordenamentos deveriam pensar em mecanismo e estratégias regulatórias que facilitem o processo de tomada de decisão do usuário. Nesse sentido[182]:

> Deve-se, contudo e concomitantemente, pensar em disposições normativas complementares que interfiram no próprio fluxo informacional, não deixando, apenas, sobre os ombros dos titulares dos dados pessoais, o fardo normativo da proteção de dados. A tutela jurídica deve ir muito além do raciocínio bifásico centrado na escolha do indivíduo em consentir ou não com tratamento dos seus dados pessoais.

Compreende-se, portanto, que o controle de tratamento tradicional por meio de proteção contratual do consumidor encontra empecilhos para o seu bom funcionamento, uma vez que seria, por excelência, um controle *ex post*[183], mediante declaração de abusividade das cláusulas dos termos de privacidade, que funcionariam como um contrato de adesão. Entretanto, a regulação da proteção de dados via extensa adjetivação do consentimento visa um controle prévio do consumidor. Dessa forma, essa proteção contratual do consumidor não deve ser vista como ideal, mas como uma medida paliativa se a causa regulatória primária, que seria o empoderamento *ex ante* do cidadão, falhar[184].

O ideal seria, portanto, pensar em uma via inversa. Ou seja, ao invés da massificação das políticas de privacidade das empresas, dever-se-ia investigar como a tecnologia poderia

[182] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 168.
[183] Ibidem, p. 173.
[184] Ibidem, p. 174.

massificar as escolhas dos consumidores sobre o trânsito dos seus dados pessoais para análise dos atores do mercado, com o objetivo de contrabalancear a estratégia regulatória de atrofiar a adjetivação do consentimento[185]. Nesse sentido, analisar-se-ão algumas ferramentas que poderiam ficar à disposição dos consumidores para a concretude dessa inversão de contexto, sem, no entanto, procurar exaurir todas elas.

4.2.1 *Do Not Track* / DNT

O *Do Not Track* (DNT) – Não Me Rastreie – é uma ferramenta que surgiu dentro da perspectiva de pensar novos meios para facilitar o controle dos dados pessoais. Essa ferramenta seria uma alternativa à necessidade de o usuário ficar aceitando ou rejeitando *cookies* e ainda correr o risco de ter algum instalado sem o seu conhecimento. Bastaria o cidadão acionar o "DNT" para que a sua escolha de aceitar ou não a coleta dos seus dados fosse exteriorizada automaticamente para todos os *sites* acessados. Essa funcionalidade seria acionada pelo próprio navegador do usuário que sinalizaria a sua opção para todas as aplicações por ele acessadas[186].

Essa ferramenta, entretanto, é objeto de muita discussão entre diversos setores empresariais, principalmente pela indústria da publicidade comportamental, e acabou enfraquecida no mercado. Dessa forma, segundo defende o autor Bruno Ricardo Bioni, como a própria autorregulação falhou para a efetivação dessa ferramenta, faz-se necessária, então, uma intervenção regulatória do Estado para concretizar o uso do DNT e empoderar o cidadão com o controle efetivo de seus dados[187]

4.2.2 *Plataform for Privacy* / P3P

A *Plataform for Privacy* – Plataforma para Preferência de Privacidade – permite os usuários, por intermédio de seus navegadores, configurarem a sua privacidade conforme a sua preferência, como selecionar quais os tipos de dados poderão ser coletados e se poderão ser compartilhados com terceiros. Dessa forma, o próprio *browser* faria uma análise automatizada

[185] Ibidem, p. 175.
[186] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 180.
[187] Ibidem, p. 182.

de todas as políticas de privacidade para verificar quais *websites* seriam compatíveis ou não com as definições pré-estabelecidas[188].

O empecilho para a disseminação do uso dessa ferramenta é a sua forma de funcionamento. Primeiro, haveria uma necessidade de os navegadores adotarem a sua funcionalidade. Segundo, todas as políticas de privacidade deveriam ser adaptadas a um formato padronizado para que a ferramenta pudesse executar um protocolo de análise semântica e sintática para a leitura dos termos de uso[189].

Nesse sentido[190]:

> Com efeito, o P3P teria potencial de tornar o fluxo informacional massificado para ambos os lados da relação de consumo do mercado informacional, já que a tecnologia permitiria aos consumidores universalizar as suas preferências de privacidade e, consequentemente, controlar seus dados pessoais sem que fosse necessária a sua leitura singular e impraticável de cada política de privacidade.

Assim, a lógica da escolha binária entre o 'concorda" ou "discorda" seria substituída pelo "consentimento granular"[191], assegurando o poder de barganha dos consumidores na troca econômica da economia de dados, fazendo com que a autodeterminação informacional do cidadão seja tão fluida quanto o trânsito de dados[192]. Entretanto, assim como ocorreu com a DNT, a ausência de ação regulatória que tornasse obrigatória a sua utilização pelos navegadores e aplicações foi determinante para o seu insucesso.

Dessa forma, o P3P seria um novo mecanismo de autodeterminação informacional que substituiria a ineficiente relação contratual realizada por meio de termos de uso, diminuindo a hipervulnerabilidade do consumidor em relação aos atores da economia digital.

---

[188] Ibidem, p. 183.

[189] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 183.

[190] Ibidem, p. 184.

[191] Nesse sentido: "O consentimento granular estabelece, portanto, limites à microeconomia dos dados pessoais, na medida em que resguarda a opção do titular em emitir autorizações fragmentadas no tocante ao fluxo de seus dados pessoais. Desta forma, uma aplicação pode oferecer inúmeras funcionalidades, cujo funcionamento demanda, indispensavelmente, uma gama de dados pessoais para a sua operacionalização. Com a ressalva do consentimento granular, o titular poderá fazer o uso de tal aplicação, determinando, de forma correlacionada, quais dados pessoais seus serão tratados de acordo com as funcionalidades que pretende fazer uso." BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 55. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso dia 17/06/2019.

[192] BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 185.

4.3 – O Futuro das Regulações Sobre o Uso de *Cookies* na União Europeia e no Brasil

4.3.1 O Novo Regulamento Europeu

Em janeiro de 2017, a Comissão Europeia publicou uma proposta de regulamento que substituiria a Diretiva 2002/58/CE. Essa proposta representa a preocupação da União Europeia com os novos desafios e paradigmas da era digital, que pretende complementar e assegurar a coerência entre a regulação no setor de comunicações eletrônicas e o Regulamento Geral de Proteção de Dados.

Dentre as mudanças trazidas pelo novo regulamento, está a simplificação das regras de utilização de *cookies*, pretendendo uma configuração mais intuitiva e acessível ao aceitar ou negar a utilização de *cookies* pelos usuários. Essa mudança confirma o reconhecimento da União Europeia da sobrecarga do consentimento dos titulares nas relações digitais.

Nesse sentido, cabe destacar o considerando nº 23 da proposta que dispõe:

> (23) Os princípios da proteção de dados desde a conceção e por defeito foram codificados no artigo 25.º do Regulamento (UE) 2016/679. Atualmente, a maioria dos programas de navegação estão configurados, por defeito, para «aceitarem todos os testemunhos de conexão». Por conseguinte, os fornecedores de software que permitam a recuperação e a apresentação de informações da Internet devem ser obrigados a configurar o software de modo a que ofereça a possibilidade de impedir o rastreio por defeito entre domínios e o armazenamento de informações por terceiros nos equipamentos terminais; este procedimento é frequentemente apresentado como «rejeitar rastreadores e testemunhos de conexão de terceiros». Os utilizadores devem dispor, por defeito, da configuração que lhes permita escolher entre diferentes níveis um conjunto de opções de privacidade, desde o nível mais elevado (por exemplo, «nunca aceitar rastreadores nem testemunhos de conexão») até ao nível mais baixo (por exemplo, «aceitar sempre rastreadores e testemunhos de conexão»), passando pelo nível intermédio (por exemplo, «rejeitartodos os rastreadores e testemunhos de conexão que não sejam estritamente necessários para fornecer o serviço explicitamente solicitado pelo utilizador» ou «rejeitar todos os rastreios entre domínios»). Estas opções podem também ser mais precisas. As predefinições de privacidade devem incluir igualmente opções que permitam ao utilizador decidir, por exemplo, se Flash, JavaScript ou outro software similar pode ser executado, ou se um sítio web pode recolher os dados de localização geográfica do utilizador ou aceder a hardware específico, como uma webcam ou um microfone. Essas predefinições de privacidade devem ser apresentadas de uma forma compreensível, objetiva e facilmente visível[193].

Assim, apesar de não impor a regularização de ferramentas como o DNT ou o P3P, nota-se uma preocupação em dar mais opções ao usuário acerca de um "consentimento granular", no qual ele pode escolher os "níveis" de aceitação ou não aceitação sem ter que analisar uma

[193] EUX-LEX. Proposta de Regulamento Relativo à privacidade e às comunicações eletrônicas. Disponível em: http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_PT.html?redirect. Acesso dia 18/06/2019.

série de termos de uso para cada *site* acessado. Portanto, a legislação comunitária europeia mostra um avanço na regulação mais eficaz de proteção de dados, garantindo cada vez mais uma verdadeira autodeterminação informacional ao cidadão.

4.2.1 O Futuro da Regulação no Brasil

A Lei Geral de Proteção de Dados Pessoais somente entrará em vigor no ano de 2020, o que torna difícil a previsão acerca da sua efetividade. Entretanto, não é absurdo afirmar que ela trará grande impacto para o funcionamento da sociedade, tendo em vista em todos os setores do mercado ocorre tratamento de dados.

Com essa nova lei, o Brasil sai do atraso em relação à proteção de dados e se junta aos outros países que possuem uma Lei Geral. Não obstante as críticas recebidas por essa norma, ela possui um relevante papel para a proteção do cidadão ao delimitar as hipóteses de uso dos dados pessoais e promover a autodeterminação informacional do indivíduo.

Entretanto, já é possível notar algumas reformas na lei. O conceito abrangente e abstrato de interesse legítimo, por exemplo, pode permitir a mitigação dos princípios e garantias previstos na lei, devendo haver uma delimitação mais exata e específica do conceito de interesse legítimo. Além disso, é preciso rever a forma com que o consentimento é tratado no âmbito digital, uma vez que a forma como está disposto na lei gera um bombardeamento de informações e termos de uso que deixa a navegação do usuário maçante e acaba inviabilizando um livre consentimento do cidadão.

CONSIDERAÇÕES FINAIS

O direito à privacidade nem sempre foi um ponto de grande relevância para os diversos ordenamentos jurídicos, sendo, muitas vezes preterido em relação ao direito patrimonial. No início do século XX, pôde-se notar o surgimento de uma maior importância para esse direito, sendo caracterizado, na época, como o "direito de ficar só", que apresentava uma concepção individualista.

Na atual sociedade da informação, os dados pessoais configuram uma nova moeda de troca. Aliado a isso, a crescente inovação tecnológica proporcionou mecanismos de coleta e tratamento de dados mais eficientes e rápidos que são capazes de criar um perfil comportamental do consumidor. Embora essa atividade traga mais conforto e facilidade para a vida dos cidadãos, o seu uso abusivo e sem regulação provoca ameaças à vida privada e íntima dos indivíduos, podendo, inclusive, criar decisões automatizadas discriminatórias que criam barreiras para as oportunidades sociais de determinada pessoa.

Dessa forma, o conceito de privacidade sofreu um processo de evolução, passando para uma nova dimensão na qual o indivíduo possui o direito de controlar as suas informações e construir a sua vida privada como entender melhor. Entretanto, o direito à privacidade permanecia preso à dicotomia público-privado e não era mais suficiente para a proteção do indivíduo no que diz respeito ao uso abusivo de suas informações.

Tendo isso em vista, criou-se uma necessidade de regulação do tratamento de dados pelo Estado. O desafio dessa regulação é a criação de medidas que proporcionem a proteção dos direitos fundamentais dos indivíduos ao mesmo tempo que garanta o desenvolvimento econômico do país. Surge, assim, um novo direito fundamental autônomo: o direito à proteção de dados pessoais.

A Europa foi a pioneira na criação de normas que visam a autodeterminação dos indivíduos em relação ao uso de seus dados pessoais. Em 1995, a União emanou a diretiva 95/46/CE, que era a norma mais moderna à época e ainda possui grande importância nos dias de hoje, uma vez que influenciou diretamente na criação do Regulamento Geral de Proteção de Dados. A Diretiva 95/46/CE previu importantes princípios para garantia da proteção de dados dos cidadãos contra o tratamento abusivo, como o princípio da transparência; da finalidade; da necessidade; da exatidão; e do consentimento.

O consentimento era o regime central dessa norma, devendo ser inequívoco, livre, informado e específico para as finalidades declaradas. Além disso, determinava que o titular tinha o direito de acesso às informações sobre dos seus dados pessoais, devendo o responsável enviar informações claras, exatas e de fácil compreensão. Também faziam parte dos direitos do titular o direito de retificação de qualquer informação errada sobre seus dados e de oposição ao tratamento de dados e decisões automatizadas.

Alguns anos depois foi emanada a diretiva 2002/58/CE, relativa à privacidade e comunicações eletrônicas. Um dos seus objetivos era a regulação do uso da ferramenta de *cookies*. Relativamente a essa ferramenta, a diretiva determinou que as entidades deveriam ter o consentimento prévio do titular para a utilização dessa ferramenta, além da necessidade de informá-los de maneira clara e completa acerca do uso de *cookies*. Por outro lado, a diretiva também previu exceções ao consentimento prévio para a utilização de *cookies* necessários para o fornecimento do serviço solicitado.

Por causa da natureza jurídica das diretivas, que exige a sua transposição para o direito interno de cada Estado-membro para gerar efeitos, diversos conflitos decorrentes de interpretações e aplicações ocorreram entre os países que compõem a União Europeia. Esse problema, somado aos avanços tecnológicos na coleta e tratamento de dados, fizeram que o Parlamento Europeu criasse um regulamento que substituísse a Diretiva 95/46/CE.

Nesse sentido, em abril de 2016 foi publicado o Regulamento Geral de Proteção de Dados que viria a substituir a Diretiva 95/46/CE em maio de 2018, ao entrar em vigor. O novo formato normativo foi necessário para padronizar e resguardar de forma mais eficiente as garantias de proteção dos dados pessoais dos cidadãos, gerando condições mais igualitárias entre os Estado-membros. Entretanto, apesar da nova regulação trazer mudanças significativas no ordenamento da União, os princípios definidos na Diretiva 95/46/CE foram recepcionados e permanecem válidos.

O Regulamento compreendeu pela interpretação extensiva do conceito de dado pessoal, considerando qualquer informação que identifique uma pessoa ou permita que ela seja identificável. Dessa forma, ao considerar os *cookies* como um dado pessoal, o Regulamento os torna sujeitos às suas diretrizes, exigindo uma adaptação da Diretiva 2002/58/CE.

O RGPD concedeu um conceito mais definido ao consentimento, agregando a ele uma extensa adjetivação. Assim, o Regulamento afirma que o consentimento deverá ser dado

mediante ato positivo e claro que indique a manifestação livre, específica, informada e inequívoca de que o titular consente com o tratamento de dados. Ao exigir um "ato positivo claro" e inequívoco da manifestação, a norma indica a necessidade de um consentimento mediante declaração escrita, inclusive em formato eletrônico ou declaração oral. Portanto, o consentimento prévio exigido pela Diretiva 2002/58/CE não pode ser tácito, uma vez que uma "omissão" não pode ser considerada uma inequívoca manifestação de vontade.

Além disso, o texto normativo ainda determina que o consentimento do cidadão deve poder ser retirado a qualquer momento, devendo ser tão fácil quanto dar. Se o titular não puder recusar ou retirar o consentimento sem ser prejudicado, o consentimento não será considerado livre e a utilização da ferramenta de *cookies* será ilegítima.

Assim, o consentimento ficou mais claro e definido com o RGPD. Entretanto, o problema da autorização limitada pela dualidade entre "permitir" e "não permitir" reside principalmente em dois fatos: a exclusão do indivíduo do mercado, uma vez que muitas empresas podem vincular os *cookies* a um bloqueio prévio que não permite o acesso daquele usuário que não aceitou; e o consentimento prévio e expresso para todas as finalidades do eventual *cookie* utilizado pode bombardear o usuário de avisos de instalação de *cookies*, tornando a navegação maçante e inviabilizando o livre consentimento, uma vez que o usuário passa a negar ou aceitar a utilização da ferramenta sem compreender do que se tratava.

O Regulamento Geral de Proteção de Dados também prevê outras formas legítimas de tratamento de dados que não apenas o consentimento. Uma dessas hipóteses é o tratamento de dados baseado no interesse legítimo do responsável pelo tratamento. Para evitar um conceito abstrato que colocasse em xeque os princípios e garantias da proteção de dados pessoais, o Regulamento se preocupou em determinar que a aplicação dos interesses legítimos levasse em conta as expectativas razoáveis dos titulares dos dados, não podendo prevalecer os seus interesses ou liberdades individuais. Dessa forma, o tratamento de dados só pode se basear no interesse legítimo se o novo tratamento for compatível com as finalidades para as quais os dados tenham sido inicialmente recolhidos.

Portanto, os critérios para a aplicação dos interesses legítimos devem assegurar a previsibilidade e compatibilidade com os interesses do titular dos dados pessoais. Cabe notar, ainda, que a aplicação da ferramenta de *cookies* sempre dependerá do consentimento prévio do usuário, conforme a Diretiva 2002/58/CE. Entretanto, o tratamento dos dados já coletados

poderá ocorrer com uma finalidade diversa daquela informada para a aplicação do *cookie*, desde que sejam respeitadas as determinações do Regulamento.

O Regulamento dispõe da possibilidade de oposição ao tratamento de dados pelo seu titular. Caso isso ocorra, o responsável poderá negar o pedido de oposição apenas quando conseguir demonstrar que existe legítimo interesse para o processamento ou que seja necessário por razões legais. Com o direito à oposição o consentimento poderia ser feito de maneira fragmentada, pois o titular poderia determinar quais dados poderiam ser tratados e de qual maneira. Entretanto, a oposição só é realizada após o consentimento, ou seja, o usuário consente com tudo e depois pode se opor. Na utilização de *cookies* isso é ainda mais difícil de ocorrer, uma vez que as empresas apresentam muitas vezes todos os *cookies* em conjunto, exigindo uma capacidade técnica superior a de um cidadão comum para distingui-los.

Dessa forma, apesar de haver outras formas de legitimação do tratamento de dados, o consentimento continua sendo a principal. Quando se trata especificamente do uso da ferramenta de *cookies*, o consentimento está inteiramente presente, devendo ser prévio, livre, inequívoco, informado e explícito. Contudo, apesar da importância do consentimento para garantir a autodeterminação informativa do cidadão em relação ao uso de seus dados, esse método por si só possui fragilidades e muitas vezes as suas adjetivações não são garantidas em sua totalidade.

O Brasil está atrasado na regulação do tratamento de dados pessoais, uma vez que a Lei Geral de Proteção de Dados Pessoais ainda não está em vigor. Entretanto, é possível encontrar fundamentos para a defesa dos dados pessoais em legislações esparsas. As mudanças sociais e tecnológicas ensejaram no desenvolvimento de um novo direito à privacidade no ordenamento jurídico brasileiro. Podemos encontrar essa tutela, por exemplo, no Código de Defesa do Consumidor que, em seu artigo 43, estabelece a tutela da privacidade do consumidor também em relação aos seus dados pessoais. Além disso, outras leis como a Lei do Cadastro Positivo e o Marco Civil da Internet introduzem regras e princípios que contribuem para a proteção dos dados pessoais e deram os primeiros passos para a redação de uma legislação específica.

A Lei Geral de Proteção de Dados foi finalmente publicada no ano de 2018 e entrará em vigor em 2020. Essa norma foi inspirada pelo Regulamento Geral de Proteção de Dados da União Europeia e carrega grande similitude em relação ao Regulamento. Entretanto, é possível encontrar algumas divergências como a falta de uma conceituação concreta e específica de interesse legítimo. Além disso, o direito à oposição a tratamento de dados baseado no interesse

legítimo só poderá ser realizado caso o interesse for contrário a lei, o que reduz a participação do titular em comparação com o Regulamento europeu. Isso gera uma maior vulnerabilidade da lei brasileira no uso da ferramenta de *cookies*, uma vez que abre brecha para o uso abusivo desse dispositivo.

Ao longo do presente trabalho foi possível analisar que mesmo prevendo outras hipóteses para o tratamento de dados, o consentimento continua sendo a principal base jurídica que justifique a legitimidade da coleta e tratamento de dados pessoais em ambos os ordenamentos. No entanto, a complexidade do fluxo informacional e seus inúmeros tores envolvidos na comercialização de dados torna o usuário muito mais vulnerável. Nesse sentido, a crença de que o cidadão conseguirá exercer a sua autodeterminação informacional em um processo racional de tomada de decisão acerca do consentimento ou não do uso de seus dados não é necessariamente correta.

No contexto do tratamento de dados, principalmente na utilização da ferramenta de *cookies*, os cidadãos são bombardeados de informações e termos de uso que deveriam ser analisados para uma tomada de decisão realmente livre e racional. Entretanto, a análise do funcionamento de cada *site* visitado é irreal, não sendo possível o cidadão ter consciência a respeito de todos eles para gerenciar as suas informações pessoais.

Ademais, o cidadão médio não tem conhecimento técnico suficiente para compreender a consequência de todas as suas atitudes e, mesmo que tenha, há uma tendência em focar nos benefícios imediatos e deixar de ponderar possíveis prejuízos futuros. Dessa forma, o cidadão deixa de tomar conhecimento acerca do tratamento de seus dados pessoais, aceitando ou recusando a utilização de *cookies* sem um real conhecimento de causa. Portanto, percebe-se que a pretensão de consentimento livre já nasce corrompida.

Para mudar esse cenário, os ordenamentos deveriam pensar em mecanismo e estratégias regulatórias que facilitem o processo de tomada de decisão do usuário e invertam esse cenário, massificando a vontade dos titulares para a análise dos *sites* visitados e não o contrário. Isso seria possível utilizando o desenvolvimento tecnológico em favor da proteção à privacidade e aos dados pessoais.

Foram, assim, apresentadas duas ferramentas que poderiam resolver esse problema, o *Do Not Track* (DNT) e o *Plataform for Privacy* (P3P). Essas ferramentas seriam uma alternativa à necessidade de o usuário ficar aceitando ou rejeitando os *cookies*. Por meio dessas ferramentas

o usuário poderia escolher negar todos os tipos de *cookies* ou selecionar qual tipo de tratamento de dados seriam permitidos, devendo os *sites* se adaptarem às escolhas dos cidadãos.

Assim, a lógica da escolha binária entre o ‘concorda” ou “discorda” seria substituída pelo “consentimento granular”, assegurando o poder de barganha dos consumidores na troca econômica da economia de dados, fazendo com que a autodeterminação informacional do cidadão seja tão fluida quanto o trânsito de dado.

Por fim, foram mencionadas as expectativas futuras das legislações na melhora da proteção de dados pessoais. A União Europeia possui uma proposta de um novo Tratado que substituirá a Diretiva 2002/58/CE que aplicará regras mais simples de utilização de *cookies*, pretendendo uma configuração mais intuitiva e acessível ao aceitar ou negar a utilização de *cookies* pelos usuários. Essa mudança confirma o reconhecimento da União Europeia da sobrecarga do consentimento dos titulares nas relações digitais

Em relação ao Brasil, por outro lado, ainda é cedo falar em um futuro da regulação da proteção de dados pessoais, visto que a Lei Geral de Proteção de Dados ainda não entrou em vigor e não é possível verificar os seus impactos. Entretanto, por meio da análise comparada com a União Europeia, pode-se perceber uma necessidade de reforma da lei para uma delimitação mais exata e específica do conceito de interesse legítimo, além de rever a forma com que o consentimento é tratado no âmbito digital, sobretudo na regulação do uso da ferramenta de *cookies*.

BIBLIOGRAFIA

ALEMANHA, *Deutscher Bundestag* , 1949, disponível em: https://www.btg-bestellservice.de/pdf/80208000.pdf.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018.

BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 55. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso dia 17/06/2019.

BIONI, Bruno Ricardo; RIBEIRO, Márcio Moretto: A transposição da dicotomia entre o público e privado. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-transposicao-da-dicotomia-entre-o-publico-e-o-privado.

BRASIL, Constituição da República Federativa de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

__, Lei nº 8.8078, de 11 de setembro de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso dia 10/06/2019.

__, Lei nº 10.406, de 10 de janeiro de 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm.

__, Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

__. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

__. PEC 17/2019, Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594.

CANOTILHO, Mariana; SILVEIRA, Alessandra. Carta dos Direitos Fundamentais da União Europeia Comentada. Coimbra, Portugal: Almedina, 2013.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Revista Espaço Jurídico. Vol. 12, nº 2. Joaçaba: Unoesc, 2011.

DUARTE, Maria Luísa. União Europeia – estática e Dinâmica da Ordem Jurídica Eurocomunitária. 1ª edição. Protugal, Coimbra: Almedina, 2011,

DUARTE, Vânia Sofia António. Protecção de Dados Pessoais na Internet: O Caso do "Direito a Ser Esquecido". Portugal: Faculdade e Direito da Universidade Nova de Lisboa, 2014. https://run.unl.pt/bitstream/10362/17212/1/Duarte_2014.pdf.

EUR-LEX. Carta dos Direitos Fundamentais da União Europeia, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.

__, Convenção 108, disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm.

__. Diretiva 2002/58/CE do Parlamento europeu e do Conselho, Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

__. Diretiva 95/46/CE do Parlamento europeu e do Conselho, considerandos 2 e 3, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT.

__. Proposta de Regulamento Relativo à privacidade e às comunicações eletrônicas. Disponível em: http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_PT.html?redirect.

__. Regulamento (UE) 2016/679 do Parlamento europeu e Conselho, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

__. Tratado de Funcionamento da União Europeia (TFUE), disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF.

__. Tratado da União Europeia, disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF.

ESPANHA, Constitución Española, disponível em: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf.

FARIAS, Cristiano Chaves de; NELSON, Rosenvald. Curso de Direito Civil 1: Parte Geral e LINDB. 15ª edição. Bahia: Editora *Jus* Podivm, 2017.

FRAZÃO, Ana de Oliveira. A Industria dos Dados Pessoais e os Data Brokers: Reflexões sobre os riscos da atuação de tais agentes no mercado de dados pessoais. Disponível em: http://anafrazao.com.br/files/publicacoes/2019-03-22-A_industria_dos_dados_pessoais_e_os_data_brokers_Reflexoes_sobre_os_riscos_da_atuacao_de_tais_agente//s_no_mercado_de_dados_pessoais.pdf.

__. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-08-30-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_Parte_I.pdf. Acesso dia 15/06/2019.

__. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – A Importância do Consentimento para o Tratamento dos Dados Pessoais, Parte III. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-09-12-A_nova_Lei_Geral_de_Protecao_de_Dados_Repercussoes_para_a_atividade_empresarial_a_importancia_do_consentimento_para_o_tratamento_dos_dados_pessoais_Parte_III.pdf.

__. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – As Demais Hipóteses para o Tratamento dos Dados Pessoais, Parte IV. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-09-20-

A_nova_Lei_Geral_de_Protecao_de_Dados_Repercussoes_para_a_atividade_empresarial_as_demais_hipoteses_de_tratamento_de_dados_pessoais_Parte_IV.pdf.

__. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial – O Direito à Oposição e à Explicação Diante de Decisões Totalmente Automatizadas, Parte XV. Disponível em: http://www.anafrazao.com.br/files/publicacoes/2018-12-06-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_o_direito_a_explicacao_e_a_oposicao_diante_de_decisoes_totalmente_automatizadas_Parte_XV.pdf.

FONTAÍNHAS, Emília Golim; ANDRADE, Francisco; AMLEIDA, José Bacelar. Do Consentimento para a Utilização de Testemunhos de Conexão (cookies). Portugal: Scientia Iuridica, Tomo LXV nº 341, 2016.

GALDINO, Natanael. Big Data: Ferramentas e Aplicabilidade. Disponível em: https://www.aedb.br/seget/arquivos/artigos16/472427.pdf.

GARFINKEL, Simon. *Database Nation: the death of privacy in the 21th Century*. California: O'Reilly Media, 2000, p. 5. *apud* MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014.

IRWIN, Luke. How the GDPR Affects Cookie Policies. Disponível em: https://www.itgovernance.eu/blog/en/how-the-gdpr-affects-cookie-policies

KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. Soft *surveillance, hard consent.* In: KERR, Ian (Ed.) *Lessons from identity trail: anonymity, privacy and identity in a networked society.* New York: Oxford University Press, 2009, p. 17 *apud* BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018, p. 147.

MALDONADO, Viviane Nóbrega, BLUM, Renato Opice. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo, Thomson Reuters, 2018.

MARTÍN, Araceli Mangas; NOGUERAS, Diego J. Liñan. *Instituciones Y Derecho de La Unión Europea*. 8ª edição. Espanha, Madrid: Tecnos, 2015.

MARTINS, Ana Maria Guerra. Manual de Direito da União Europeia. 2ª edição. Portugal, Coimbra, 2017.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: Linhas gerais de um novo direito fundamental. 1ª ed. São Paulo: Saraiva, 2014.

MIRANDA, Leandro Alvarenga. A Proteção de Dados Pessoais e o Paradigma da Privacidade. 1ª ed. São Paulo: All Print Editora, 2018.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoas: Comentários à Lei nº 13.709/2018 (LGPD). 1ª ed. São Paulo: Saraiva, 2018.

PORTUGAL, Constituição da República Portuguesa, disponível em:

https://www.parlamento.pt/Legislacao/paginas/constituicaorepublicaportuguesa.aspx.

QUEIROZ, Anderson Apolônio Lira. A Invasão de Privacidade na Internet: um Modelo de Boas Práticas e uma Proposta Interativa de Proteção da Privacidade por Meio dos Cookies. 2011. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011.

RODOTÁ, Stefano. A Vida na Sociedade da Vigilância. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O Direito à Proteção de Dados Pessoais e a Privacidade. Curitiba: Revista da Faculdade de Direito – UFPR, nº53, 2011.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina. Marco Civil da Internet: Jurisprudência Comentada. 2ª tiragem. São Paulo: Revista dos Tribunais, 2018.

ZANON, João Carlos. Direito à Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2013, p. 63, *apud* BIONI, Bruno Ricardo. Proteção de Dados Pessoais – A função e os limites do consentimento. 1ª ed. Rio de Janeiro: Editora Forense, 2018.