UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
GRADUAÇÃO EM DIREITO

LUCAS MATHEUS FERNANDES LOBO

DA EFETIVIDADE DO CONSENTIMENTO NA LGPD PARA A GARANTIA DOS DIREITOS FUNDAMENTAIS À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

FORTALEZA
2022

LUCAS MATHEUS FERNANDES LOBO

DA EFETIVIDADE DO CONSENTIMENTO NA LGPD PARA A GARANTIA DOS DIREITOS FUNDAMENTAIS À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Monografia apresentada ao curso de Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Emmanuel Teófilo Furtado Filho.

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

L783e Lobo, Lucas Matheus Fernandes.
Da efetividade do consentimento na lgpd para a garantia dos direitos fundamentais à privacidade e à proteção de dados pessoais na internet / Lucas Matheus Fernandes Lobo. – 2022.
68 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2022.
Orientação: Prof. Dr. Emmanuel Teófilo Furtado Filho.

1. Lei Geral de Proteção de Dados. 2. Consentimento na Lei Geral de Proteção de Dados . 3. LGPD e Direito Fundamental à Privacidade e à Proteção de Dados. 4. Direito Fundamental à Privacidade e Direito Fundamental à Proteção de Dados Pessoais na internet. 5. Efetividade do Consentimento na LGPD. I. Título.
CDD 340

LUCAS MATHEUS FERNANDES LOBO

DA EFETIVIDADE DO CONSENTIMENTO NA LGPD PARA A GARANTIA DOS DIREITOS FUNDAMENTAIS À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Monografia apresentada ao curso de Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Aprovada em: 11 / 11 / 2022.

BANCA EXAMINADORA

_____
Prof. Dr. Emmanuel Teófilo Furtado Filho (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Me. Matheus Casimiro Gomes Serafim
Universidade Federal do Ceará (UFC)

_____
Ma. Vanessa de Lima Marques Santiago Sousa
Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

Aos meus pais, Antônio e Aurilene, que são os melhores pais que eu poderia querer. Cada um ao seu modo, ambos me ensinaram todos os valores de honestidade, bondade e humildade, que me motivam todos os dias a tentar ser uma pessoa melhor. Obrigado por lutarem desde cedo e fazerem o impossível para que pudessem proporcionar uma vida melhor a mim e aos meus irmãos. Sou extremamente grato por todos os ensinamentos que vocês me deram e por sempre fazerem parte de todos os ciclos da minha vida. Tenho sempre em vocês um exemplo a ser seguido. Vocês são a base de toda a minha vida.

Aos meus avós, Paulo, Laura, Dalci e Tereza, por terem ajudado na minha criação e terem feito parte no meu desenvolvimento como ser humano. Mesmo que não tenha tido o tempo que gostaria com todos, sou muito grato pela forma como vocês cuidaram de mim.

Aos meus irmãos, Paulo e Gabriela. Vocês simplesmente conseguiram cumprir para mim o papel de pai/mãe, irmão/irmã e amigo/amiga. Vocês realizaram um grande papel na minha criação e na minha formação como ser humano. Tenho a maior sorte do mundo de terem vocês ao meu lado, que sempre contribuíram com dicas e conselhos para a minha vida e para o meu futuro. Vocês sempre me proporcionaram muita alegria e diversão, além de sempre estarem ao meu lado em todos os momentos em que precisei de vocês, sendo fundamentais em todos os ciclos da minha vida.

À minha namorada, Letícia Melo, que é a menina mais incrível que eu já conheci e o melhor presente que a vida me deu. Obrigado por despertar o melhor em mim e por me ajudar em tudo o que eu precisar. Você é um exemplo de pessoa alegre, divertida, inteligente, esforçada, humilde e bondosa. É minha fonte de inspiração diária para que eu possa conquistar meus objetivos profissionais e pessoais. Quero muito passar o restante da minha vida ao seu lado.

Ao João, meus professores e amigos de faculdade, que auxiliaram nessa importante etapa da minha vida e contribuíram para que eu pudesse percorrer os últimos anos com leveza e tranquilidade.

E por fim, a todos aqueles que acreditam no poder da educação e que utilizam essa arma para ajudar a sociedade, e não apenas para satisfações pessoais. A todos aqueles que acreditam em um mundo melhor, mais justo e que lutam todos os dias para impactar positivamente na vida do outro. Esse é o grande propósito disso tudo: ajudar as outras pessoas.

“Cada suspiro que você der, cada movimento que você fizer, cada laço que você quebrar, cada passo que você der eu estarei te observando.” (STING, Gordon Matthew Thomas Summer. The Police. *Every Breath You Take*. Londres. A&M. 1983. 4:14 min. Tradução nossa).

RESUMO

O presente trabalho buscou realizar um panorama e uma análise sobre a privacidade e a proteção de dados no Brasil no ambiente online, notadamente com questões relacionadas à efetividade do consentimento advindo da Lei Geral de Proteção de Dados. O objetivo dessa pesquisa é entender o histórico e a conceituação do direito fundamental à privacidade e à proteção de dados pessoais, de modo que, a partir disso, seja possível compreender a evolução desses direitos no ambiente online com a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados. Com o entendimento sobre a LGPD, passa a ser possível averiguar seus pontos mais importantes, especialmente a ideia do consentimento, uma das premissas basilares da Lei 13.709/2018. Logo, analisa-se a efetividade desse consentimento, com averiguação de seus aspectos positivos e negativos. Por fim, o intuito é encontrar formas de garantir uma efetividade maior do consentimento, de modo a assegurar o respeito aos direitos fundamentais da privacidade e da proteção de dados pessoais. Acerca da metodologia, o procedimento adotado foi o bibliográfico, com a utilização de livros e artigos científicos. Quanto à abordagem, pode-se afirmar um forte viés qualitativo, tendo em vista o caráter interpretativo da LGPD. Em relação aos objetivos, pode ser classificada como exploratória, pois busca proporcionar uma maior familiariedade com o tema.

Palavras-chave: Privacidade. Proteção de Dados. Lei Geral de Proteção de Dados. Consentimento. Internet.

ABSTRACT

The present work sought to carry out an overview and analysis of privacy and data protection in Brazil in the online environment, notably with issues related to the General Data Protection Act defined on data protection. This research is to understand the history and conceptualization of the fundamental right to privacy and the protection of personal data, so that, from this, it is possible to understand the evolution of these rights in the online environment with the Carolina Dieckmann Law, the Marco Civil da Internet and the General Data Protection Act. With the understanding of the LGPD, it becomes possible to ascertain its most important points, especially an idea of consent, one of the basic premises of Law 13,709/2018. Then, its aspects of contact are analyzed, with positive and negative verification. Finally, the objective is to guarantee greater protection of consent, in order to guarantee respect for the fundamental rights of privacy and protection of personal data. Regarding the methodology, the procedure adopted was the bibliographical one, with the use of books and scientific articles. As for the approach, a strong qualitative bias can be affirmed, in view of the interpretative nature of the LGPD. Regarding the objectives, it can be classified as exploratory, as it seeks to provide greater familiarity with the theme.

Keywords: Privacy. Data Protection. General Data Protection Act. Consent. Internet.

LISTA DE FIGURAS E TABELAS

SUMÁRIO

1 INTRODUÇÃO

O direito fundamental à privacidade passou por várias transformações ao longo do tempo. Inicialmente era visto como uma liberdade negativa, marcado pelo direito de ser deixado sozinho e de não sofrer intromissões em sua vida privada. Contudo, ao longo do tempo, com a coleta massiva de dados das pessoas, foi surgindo um direito de que os indivíduos tivessem controle sobre quais dados estariam sendo coletados, além de uma prerrogativa de autorizar ou não o armazenamento e o envio para terceiros. Desse modo, o direito à privacidade foi passando a ter também um caráter positivo, relacionado a uma postura ativa dos indivíduos de exercerem controle sobre seus próprios dados. Com a evolução dessa sistemática, foi progressivamente surgindo um novo direito autônomo, o direito fundamental à proteção de dados.

Assim, os Estados foram gradativamente legislando sobre o assunto, estabelecendo diretrizes, de modo a regular o tratamento de dados das pessoas, especialmente na internet, local de intensa coleta de dados e de uso de algoritmos que monitoram a atividade online dos indivíduos, para, entre outros motivos, enviar anúncios personalizados para eles.

No Brasil, o grande marco legislativo ocorreu com a Lei 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o propósito de garantir uma ampla proteção aos indivíduos e proteger os seus direitos fundamentais.

Para cumprir seus objetivos, a LGPD busca conferir ao próprio indivíduo o poder de decidir se terá ou não seus dados tratados. Baseada na ideia da autodeterminação informativa, a LGPD confere grande importância para o consentimento do usuário. Assim, o tratamento dos dados depende da concordância do próprio titular dos dados, que tem o poder de negar o fornecimento de suas informações.

Partindo dessa premissa, a ideia do presente trabalho é analisar, além do direito à privacidade e à proteção de dados pessoais, a LGPD e a ideia do consentimento, averiguando de que modo essa política de tratamento pode ou não ser efetiva para a tutela dos direitos dos indivíduos.

2. DIREITO FUNDAMENTAL À PRIVACIDADE

É natural do comportamento humano o interesse pelo outro, seja para obter algum benefício próprio a partir dele, seja apenas para saciar sua curiosidade. Contudo, também é natural dos seres humanos o desejo de que outras pessoas não saibam sobre alguns aspectos da sua vida. Nesse caso, estamos diante de um conflito de interesses entre o público e o privado.

Nessa tentativa de proteger a esfera privada dos indivíduos, surge a ideia do direito à privacidade, trabalhada por vários legisladores em vários países do mundo ao longo da história.

O direito brasileiro, por sua vez, não se mostra alheio a essa realidade, consagrando o direito fundamental à privacidade como um dos direitos da personalidade, estando expresso no art. 5º, inciso X, da Constituição Federal de 1988, nos seguintes termos: ‘’ 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’’ (BRASIL, 1988).

Para uma melhor compreensão sobre o tema, vamos a um breve histórico sobre o direito à privacidade, para então entendermos melhor como esse direito fundamental pode estar ainda mais ameaçado na contemporaneidade, com o desenvolvimento tecnológico e a utilização dos dados dos indivíduos na internet.

2.1 Aspectos Históricos

Os primeiros registros da ideia de privacidade remontam a tempos bastante antigos, com o desenvolvimento das primeiras grandes sociedades. Na antiguidade clássica já havia a distinção entre a vida pública e a vida privada. Cancelier (2017) explica que na Grécia havia a esfera da *pólis*, sendo comum a todos os cidadãos livres e vinculada à ideia de política, e a esfera do *oikos*, relativa ao indivíduo e relacionada à ideia de família, propriedade da família e casa.

Na Idade Média, iniciou-se um processo de isolamento, especialmente nas famílias mais nobres, na medida em que a privacidade passou a ser cada vez mais valorizada e um costume mais praticado (DONEDA, 2006, p.125, apud CANCELIER, 2017, p. 215). Foi nesse contexto que as questões relativas ao ambiente familiar passaram a se tornar mais relevantes para a comunidade.

De acordo com Cancelier (2017), com o declínio do feudalismo e a ascensão da burguesia como classe social dominante, a ideia de individualidade foi ainda mais

potencializada, destacando-se como uma forma de expressão da personalidade. Desse modo, a ideia principal era a existência de um local que possibilitasse a diferenciação do indivíduo em relação à sociedade.

Portanto, pode-se afirmar que a privacidade começou a ter mais importância na Idade Média, passando na Idade Moderna e Contemporânea a ser ainda mais enaltecida, constituindo-se como um dos mais importantes direitos dos indivíduos. Dessa forma, não tardou para que juristas e intelectuais começassem a invocá-la.

O grande marco ocorreu nos Estados Unidos, em 1890, quando os advogados Samuel Dennis Warren e Loius Dembitz Brandeis publicaram um artigo na *Harvard Law Review*, intitulado *Right to privacy*, ou Direito à Privacidade, em tradução livre. Eles estavam incomodados com o tratamento da sociedade e da mídia em relação à vida privada das pessoas. Samuel Warren sofria constantemente violações à sua intimidade, especialmente por seu casamento com Mabel Bayard, filha do senador Thomas F. Bayard. Os autores, então, analisaram várias decisões da Suprema Corte dos Estados Unidos relacionadas a direitos autorais, difamação e privacidade, defendendo, por fim, que as Cortes reconhecessem *o right to privacy,* ou direito à privacidade.

Os destacados intelectuais ainda prestaram grande auxílio para a compreensão desse direito, diferenciando-o do direito à proteção da honra. Embora sejam semelhantes, o direito à honra protege o indivíduo especialmente contra mentiras ou fatos capazes de comprometer sua reputação e sua estima perante a sociedade. O direito à privacidade, por sua vez, é ainda mais amplo e busca a proteção contra alegações e fatos em geral que o indivíduo simplesmente não tem interesse em compartilhar com a sociedade.

Um dos mais importantes momentos para o direito à privacidade ocorreu com a Declaração Universal dos Direitos Humanos (DUDH), proclamada pela Assembleia Geral das Nações Unidas, em 10 de dezembro de 1948, em um contexto no qual o mundo ainda estava chocado com vários direitos fundamentais violados durante a Segunda Guerra Mundial (1939-1945). Assim, o direito à privacidade na DUDH foi consagrado no art. XII nos seguintes termos:

> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (ONU, 1948)

O mesmo texto foi inserido também no art. 11 da Convenção Americana sobre Direitos Humanos, no Pacto de São José da Costa Rica, de 22 de novembro de 1969, ratificado pelo Brasil em 25 de setembro de 1992.

A positivação do direito à privacidade no Brasil somente ocorreu com a

promulgação da Constituição Federal de 1988, que o consagrou como um direito fundamental e uma cláusula pétrea no art. 5º da Magna Carta, nos seguintes termos:

> 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; (BRASIL, 1988).

A legislação infraconstitucional, especialmente a civilista, também se mostra bastante preocupada com o direito à privacidade. O art. 21 do Código de Direito Civil de 2002 também traz esse relevante direito fundamental, conforme se expõe abaixo:

> 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. (BRASIL, 2002).

Mesmo com todos esses avanços obtidos nos últimos anos, é inegável que a proteção à privacidade das pessoas ainda restou deficitária no contexto da rede mundial de computadores, tendo em vista que todos esses dispositivos acima citados são muito genéricos e possuem natureza essencialmente principiológica, e, embora sejam extremamente relevantes, não conseguem por si só darem conta da complexidade do ambiente digital.

Sendo assim, houve a necessidade de criação de legislações específicas para concretizar e dar efetividade ao direito fundamental à privacidade, conforme se verá mais adiante neste presente trabalho.

2.2 Conceituação

Feita a explanação histórica acerca do direito à privacidade, cabe agora entender, efetivamente, do que se trata tal prerrogativa. Antes de tudo, porém, faz-se necessário o entendimento acerca da diferença entre esfera individual e esfera privada.

A esfera individual consiste basicamente na proteção do nome e da reputação contra agressões e ataques difamatórios. A esfera privada, por outro lado, está relacionada à individualidade, a estar sozinho, ao direito de não sofrer intromissões alheias em sua paz de espírito, perturbando sua tranquilidade (COSTA JÚNIOR, 2004, p. 28, apud VIEIRA, 2007, p. 22). Desse modo, relacionando com o que foi dito mais acima, o direito à honra está vinculado

à esfera individual, enquanto o direito à privacidade propriamente dito está ligado à esfera privada.

Assim, embora não haja uma conceituação definitiva de direito à privacidade, entendemos que ele esteja relacionado ao direito subjetivo que todo indivíduo tem de evitar intromissões de terceiros em sua esfera privada, tendo então controle sobre suas informações de caráter pessoal.

Gilmar Mendes expressa a importância do direito à privacidade nos seguintes termos:

> A reclusão periódica à vida privada é uma necessidade de todo homem, para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traçar metas. (MENDES, 2022, p.672)

Portanto, estar sozinho consigo mesmo e ter a prerrogativa de não sofrer intromissões inoportunas de terceiros consiste em um dos principais direitos do ser humano, fazendo parte, inclusive, de sua formação pessoal. O fato de vivermos em sociedade não impede que tenhamos a vantagem de não sermos importunados por terceiros.

Atualmente esse direito é ainda mais relevante, na medida em que sua violação fere gravemente toda a esfera privada do indivíduo. Antigamente, com a dificuldade de difusão de informações, um indivíduo que teve sua vida privada exposta sem autorização era afetado geralmente apenas na esfera local, para seu círculo de conhecidos ou no máximo para algumas centenas de outras pessoas.

Entretanto, com a popularização da internet e a difusão de computadores e aparelhos de celular, por exemplo, a comunicação e a difusão da informação ocorrem hoje em velocidades nunca antes vistas. Logo, uma simples violação de uma informação concernente à privacidade de uma pessoa tem a capacidade de afetar toda a sua vida, pois milhões de pessoas em centenas de países do mundo podem ficar sabendo de algo que apenas o indivíduo que sofreu a violação deveria saber.

Apenas a título de exemplificação, a violação à vida privada de Samuel Warren, no final do século XIX, embora tenha trazido impactos significativos em sua esfera pessoal, chegou ao alcance apenas de parte pequena da sociedade americana no período. Por outro lado, a violação de fotos íntimas da atriz norte-americana Jennifer Lawrence, que ocorreu em 2014, certamente causou um impacto na sociedade muito maior, tendo em vista que milhões de

pessoas ao redor do mundo tiveram acesso a tais arquivos.

Nesse sentido, deve-se destacar que atualmente o direito à privacidade deve ser levado ainda mais a sério pelas autoridades, diante das consequências catastróficas que sua violação pode gerar para a vida dos indivíduos afetados.

2.3 Direito à privacidade e Direito à intimidade

Após essa conceituação acerca do direito à privacidade, faz-se necessário estabelecer a diferença entre direito à privacidade e direito à intimidade, motivo de confusão para muitas pessoas.

Acerca da diferença, pode-se afirmar que o direito à privacidade é mais geral e amplo, enquanto o direito à intimidade é mais restrito e específico. Assim, o segundo está inserido dentro do primeiro, tendo em vista que o direito à intimidade está relacionado ao íntimo de cada indivíduo, seus segredos, aquilo que está em seu interior, guardado apenas para si mesmo. Trata-se de sua consciência, seus pensamentos, sendo a esfera mais reservada de uma pessoa. O direito à privacidade, por outro lado, é mais geral, abarcando relações menos íntimas, como trabalhistas, comerciais e profissionais. Desse modo, são conceitos relacionados, mas que se relacionam. Gilmar Mendes diferencia os dois conceitos nos seguintes termos:

> O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas. (MENDES, 2022, p.669)

Nesse sentido, imprescindível citar que na internet tanto a privacidade quanto a intimidade das pessoas estão suscetíveis de violação. A primeira, por ser mais ampla e geral, tem a tendência de ser mais violada. No entanto, a segunda também pode ser exposta. Basta pensarmos, por exemplo, em conversas confidenciais de um indivíduo sendo vazadas em redes sociais.

Destarte, neste trabalho, quando estivermos abordando sobre direito à privacidade, também estamos incluindo por tabela o direito à intimidade, até porque é muito difícil dissociá-los por completo. Ademais, a Lei Geral de Proteção de Dados, que analisaremos mais adiante, possui o propósito de defender tanto o direito à privacidade quanto o direito à intimidade dos indivíduos.

Concluída essa análise sobre a privacidade, faz-se necessário entender que, com o desenvolvimento tecnológico, o direito à privacidade não foi mais se mostrando capaz de

proteger totalmente o indivíduo, tendo em vista o recolhimento e o tratamento massivo de dados das pessoas realizados por Estados e empresas. Desse modo, para uma proteção mais completa das pessoas, houve cada vez mais o desenvolvimento da ideia de um direito fundamental à proteção de dados, que será melhor trabalhado a seguir.

3. DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Com o passar dos anos, o direito à privacidade, analisado no tópico anterior, foi ficando cada vez mais complexo, à medida que ocorriam avanços tecnológicos e difusão cada vez mais acelerada de informações.

A ideia de privacidade defendida por Samuel Warren e Loius Brandeis era essencialmente uma liberdade negativa, com um caráter predominantemente individualista. Tratava-se, na grande maioria das vezes, de um direito de ser deixado só, de não ser importunado e de não sofrer intromissões de terceiros em sua vida privada, sejam eles o Estado, a imprensa ou outros indivíduos. Contudo, essa visão de privacidade, adequada para o contexto do mundo na época, passou a ficar cada vez mais obsoleta e inapropriada para garantir a efetiva proteção da vida privada dos indivíduos. A mudança de funcionamento do Estado, o avanço tecnológico e o desenvolvimento da internet fizeram com que cada vez mais as pessoas tivessem seus dados coletados por terceiros.

Primeiramente, os Estados Nacionais passaram a armazenar dados e informações sobre os indivíduos de forma mais ostensiva. Os censos foram ficando mais comuns e completos; empresas estatais foram criadas para prestar serviços públicos; cartórios passaram a atuar com muito mais eficiência e efetividade; a receita federal foi se desenvolvendo para rastrear com mais precisão a renda dos habitantes etc. Todo esse aprimoramento da máquina pública, sob a justificativa de gerenciar políticas para melhorar a qualidade de vida da população, fez com que o Estado tivesse muito mais dados e informações sobre as pessoas dos países.

As empresas não ficaram para trás, pois houve a difusão de cadastro dos clientes, que forneciam seu endereço e seus dados para contato, em troca de obter descontos e promoções exclusivas.

Com o desenvolvimento dos computadores e da internet, que começou efetivamente a partir da década de 70 do século XX, mas principalmente no decorrer da década de 90 do mesmo século, a coleta de dados foi elevada para um nível sem precedentes.

Empresas criaram sites e redes sociais que passaram a coletar diversos dados dos indivíduos, como endereço, número de telefone celular, e-mail, etnia, sexo, orientação sexual, dentre diversas outras informações. Atualmente, sites conseguem rastrear a localização das pessoas e saber com precisão os locais que visitaram. A coleta de dados e informações hoje diz respeito também à forma como se utiliza a internet. Os algoritmos de sites e redes sociais rastreiam a atividade online, de modo a entender o comportamento e, a partir disso, enviar

anúncios direcionados e personalizados, por exemplo.

Dessa forma, fica mais claro entender como atualmente o direito à privacidade do século XIX não se aplica com precisão à modernidade, tendo em vista que há a coleta excessiva de dados, especialmente no ambiente virtual. Assim, além do direito à privacidade, estamos diante de um direito fundamental à proteção de dados.

3.1 Aspectos Históricos

Como a coleta de dados ficou mais comum apenas no século XX, as legislações sobre proteção de dados eram bastante escassas. As primeiras ocorreram apenas na década de 70, em decorrência da necessidade de regulamentação por conta da introdução do processamento eletrônico de dados nas empresas privadas e nas administrações públicas em parte da Europa e nos Estados Unidos.

Assim, surgiram leis em diversos países, como Suécia e Alemanha. Laura Schertel Mendes (2014) analisou bem a situação:

> São exemplos de normas da primeira geração, no âmbito europeu, as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, foram aprovados nesse mesmo período o Fair Credit Reporting Act (1970), com foco na regulação dos relatórios de crédito dos consumidores, e o Privacy Act (1974), aplicável à administração pública. (MENDES, 2014, p.45)

Desse modo, essas legislações foram específicas para regular a coleta e o tratamento de dados que ocorriam nessas corporações, mas não havia ainda a ideia consolidada de um direito fundamental à privacidade.

No entanto, ainda na década de 70 começaram a surgir os primeiros dispositivos constitucionais que versavam sobre a proteção de dados. Os grandes marcos foram a Constituição Portuguesa de 1976 e a Constituição Espanhola de 1978. O artigo 35 da Constituição Lusa abordou sobre a proteção de dados nos seguintes termos:

> 1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
> 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
> 3. É proibida a atribuição de um número nacional único aos cidadãos. (PORTUGAL, 1976)

Desse modo, podemos constatar que a ideia de um direito à proteção de dados foi

bem introdutória, se limitando a aspectos bem específicos. Com o passar dos anos, o desenvolvimento da proteção de dados se deu mais por decisões específicas de tribunais europeus, que buscavam tutelar esse direito de forma pontual.

Uma das mais célebres decisões ocorreu em 1983, no Tribunal Constitucional Alemão, que declarou a inconstitucionalidade da Lei do Censo no país, reafirmando que os indivíduos têm direito à autodeterminação informativa, defendendo a ideia do controle do indivíduo no processamento dos seus dados.

Contudo, o grande marco da proteção de dados na Europa ocorreu com a assinatura do Regulamento Geral sobre a Proteção de Dados (RGPD), ou *General Data Protection Regulation* (GDPR), assinado em 14 de abril de 2016 e implementado em 25 de maio de 2018. Com ele, foi efetivada em solo europeu a proteção de dados dos habitantes da União Europeia, que passaram a ter um código completo versando sobre princípios, diretrizes, direitos e deveres para o tratamento e a regulação de dados.

No Brasil, o marco definitivo foi com a implementação da Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018, e entrou em vigor dia 14 de agosto de 2020.

A LGPD, que é o foco do presente trabalho e que será melhor destrinchada mais adiante, é bastante semelhante com a RGPD, e busca conferir maior segurança para o tratamento de dados realizado no território nacional.

3.2 Positivação na Constituição de 1988

Embora a Lei Geral de Proteção de Dados tenha sido publicada em 2018, não havia ainda no ordenamento jurídico a consolidação da ideia de que a proteção de dados consiste em um direito fundamental dos indivíduos. Decerto, grande parte da doutrina já entendia que a proteção de dados era um direito implícito presente na Constituição Federal de 1988.

O jurista Ingo Wolfgang Sarlet (2022) na obra Estudos Sobre Proteção de Dados Pessoais defendeu que a proteção de dados, uma vez associada ao princípio da dignidade da pessoa humana, do direito ao livre desenvolvimento da personalidade, do direito geral de liberdade, assim como os direitos à privacidade e à intimidade, pode ser entendida também como um direito fundamental implícito.

No entanto, o questionamento acerca do caráter do direito à proteção de dados acabou de vez com a Emenda Constitucional 115/2022, de relatoria da senadora Simone Tebet (MDB- MS), que acrescentou ao art. 5º o inciso: ‘’LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.’’ (BRASIL, 1988).

Dessa forma, de modo definitivo, a proteção de dados passou a ser um direito fundamental, devidamente positivada no texto constitucional como uma cláusula pétrea, devendo ser respeitada. Assim, o legislador foi bastante preciso, tendo em vista a grandiosa importância que a proteção de dados tem na vida de milhões de brasileiros.

Vamos agora partir para a análise infraconstitucional da proteção de dados e da privacidade no ambiente digital.

4. PRIVACIDADE E PROTEÇÃO DE DADOS NA INTERNET

Antes mesmo da positivação da proteção de dados como um direito fundamental, diversas leis procuraram dar mais segurança e privacidade para os indivíduos. Vamos a uma análise das principais.

4.1 Lei Carolina Dieckmann

No âmbito do histórico da proteção de dados no Brasil, imprescindível citar a Lei n. 12.737, de 30 de novembro de 2012, mais conhecida como Lei Carolina Dieckmann, que altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal) para abordar sobre a tipificação criminal de delitos informáticos.

Sua denominação extraoficial tem por base uma invasão cibernética ocorrida em um dispositivo da atriz Carolina Dieckmann em 2012. De acordo com informações do portal de notícias UOL (2012), os hackers aproveitaram que ela preencheu um formulário na internet e tiveram acesso às suas senhas, fizeram uma cópia das fotos íntimas da atriz e as hospedaram em um site de fora do país.

Dentro desse contexto, foi sancionada a Lei Carolina Dieckmann, que adicionou o art. 154-A ao código penal nos seguintes termos:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 2012)

Embora o caráter brando da pena tenha sido criticado por especialistas, como Renato Opice Blum, presidente do Conselho de Tecnologia da Informação da Fecomércio-SP (Federação dos Comércios de Bens, Serviços e Turismo do Estado de São Paulo), o fato é que a Lei n. 12.737/2012 constitui um marco para a proteção de dados no Brasil, buscando defender a privacidade e a intimidade do usuário na internet.

No entanto, destaca-se que a Lei Carolina Dieckmann abordou apenas as invasões de dispositivos eletrônicos ou de registros contidos na rede mundial de computadores, sendo necessário, ainda, uma legislação mais completa, ampla e geral sobre a regulação do uso da internet no Brasil. Foi com base nessa necessidade que surgiu o Marco Civil da Internet.

4.2 Marco Civil da Internet

A Lei n. 12.965, de 23 de abril de 2014, também conhecida como Marco Civil da Internet, dispõe sobre princípios, garantias, direitos e deveres para a utilização da Internet no Brasil.

Claramente preocupada com a proteção de direitos fundamentais, a referida lei trouxe logo no seu art. 3, incisos II e III, como princípios para a utilização da internet no Brasil, dentre outros, a ‘’proteção da privacidade’’ e a ‘’proteção dos dados pessoais, na forma da lei’’. Fiorillo (2015) destaca que, antes de ser entendida como um princípio específico relacionado ao uso da internet no Brasil, a proteção da privacidade é um princípio previsto na Constituição Federal de 1988 no seu art. 5, X, o qual indica que a vida privada das pessoas é inviolável, sendo assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

O art. 7 é ainda mais completo acerca da garantia a esses direitos. No primeiro inciso temos a ‘’inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação’’, no segundo, ‘’inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei’’, no terceiro, ‘’inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial’’.

Além do mais, o inciso VII aborda acerca do não fornecimento de dados, salvo no caso de consentimento livre, expresso e informado ou nas hipóteses previstas em lei. Desse modo, temos que esse dispositivo implica que a regra é a do não fornecimento dos dados. Entretanto, ele mesmo já traz hipóteses em que essa regra seria flexibilizada, como nos casos de consentimento livre, expresso e informado, e também nos casos previstos em lei.

Em relação ao inciso VIII aborda a questão da transparência acerca do tratamento dos dados coletados. Já em relação ao inciso IX vemos a importância do consentimento expresso acerca do tratamento dos dados, que deverá ser destacado das demais cláusulas contratuais.

Assim, observa-se claramente que no Marco Civil da Internet já havia uma preocupação do legislador acerca da proteção aos direitos fundamentais da privacidade e da proteção de dados, muito antes desse último ser positivado pelo texto constitucional com a emenda 115/2022.

Além do mais, é possível perceber desde já o enfoque no consentimento do usuário como norteador da proteção de dados no ambiente virtual, com ênfase em seu destaque das

demais cláusulas contratuais e sempre observadas suas características centrais, quais são, o seu caráter livre, expresso e informado.

Veja-se a seguir os enunciados do art. 7 com os incisos acima referenciados:

> 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;
> (...)
> 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; (BRASIL, 2014)

No art. 8 do Marco Civil da Internet, fica-se entendido que ‘’ a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet” (BRASIL, 2014). Fiorillo (2015) mais uma vez destaca a intrínseca relação entre o marco regulatório e a Constituição Federal:

> O conteúdo do art. 8 está amplamente comentado em face do que aduzimos anteriormente e, uma vez mais, deve necessariamente ser interpretado em face dos fundamentos e objetivos indicados nos princípios fundamentais de nossa Constituição Federal (arts. 1º e 3º da CF). (FIORILLO, 2015, p.127)

O art. 10, por sua vez, reforça ainda mais a proteção de dados dos usuários, dos registros de conexão e comunicações. No caput do referido artigo temos:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. (BRASIL, 2014)

O art. 16, incisos I e II do Marco Regulatório reforça o direito à privacidade e destaca o relevante papel do consentimento nos seguintes termos:

> Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados

> tenha consentido previamente, respeitado o disposto no art. 7º; ou
> II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. (BRASIL, 2014).

Fiorillo (2015) destaca também o importante papel do consentimento:

> Assim o consentimento, seja como manifestação de vontade153 favorável à realização de um ato jurídico, indispensável para sua formação e validade, seja como ato volitivo (que provém da vontade) pelo qual se declara que não há oposição a uma ação cuja iniciativa foi tomada por outrem é INDISPENSÁVEL não só no âmbito do art.16, mas em face de todo o regime jurídico definido no Capítulo III da Lei n. 12.965/2014 (Da Provisão de Conexão e de Aplicações de Internet), sendo certo que o inciso II do art. 16 deverá ser interpretado em face do critério aqui referido e em harmonia com a razão de ser de regime constitucional fundado em Estado DEMOCRÁTICO de Direito. (FIORILLO, 2015, p.129).

Embora tenha constituído significativo avanço acerca do tratamento de dados e no uso da internet no Brasil com vistas à proteção a direitos fundamentais, o Marco Civil da Internet também é alvo de pesadas críticas, especialmente no tocante à responsabilização por danos decorrentes de conteúdo gerado por terceiros, seção que abrange os arts. 18 a 21 da referida lei.

Na verdade, quis o legislador conferir um regime especial de proteção, com vistas a assegurar a liberdade de expressão e coibir a censura. Todavia, esse trecho da Lei nº 12.965/2014 claramente destoa do restante do Marco Regulatório, representando uma mudança repentina de perspectiva no tocante à proteção aos direitos da privacidade e da proteção de dados dos usuários. Observa-se o art. 18:

> Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. (BRASIL, 2014).

Fiorillo (2015) destaca que a regra geral de solidariedade, indicada no art. 3º, I, da Constituição Federal de 1988, é uma das principais fontes de interpretação da lei para o uso da internet no Brasil, mas que o art. 18 do Marco Civil da Internet a afronta flagrantemente:

> Assim, em decorrência da regra geral de solidariedade, imposta no âmbito da interpretação da lei para o uso da internet no Brasil, ou seja, em face de interpretação constitucional indicada no art. 3º, I, da Carta Magna e já comentada anteriormente, fica ao que tudo indica bem clara a inconstitucionalidade do art.18, uma vez que o provedor de conexão à internet, ao contrário do que tentar impor o art.18, poderá sim ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros, sendo certo que referida responsabilidade será solidária (provedor de conexão e terceiros) (FIORILLO, 2015, p.134).

O art. 19 estabelece restrições para a responsabilização nos seguintes termos:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial

> específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014).

Observa-se com esse dispositivo uma clara desproteção ao usuário e a possibilidade de uma impunidade para quem é responsável pelo dano. Fiorillo (2015) também fez severas críticas a esse dispositivo:

> Por outro lado, também tentando ao que tudo indica induzir em erro o intérprete e invocando direitos constitucionais deslocados de sua adequada interpretação sistemática ("com o intuito de assegurar a liberdade de expressão e impedir a censura"), procuram o art. 19 e seus parágrafos estabelecer condicionamentos infraconstitucionais aos direitos constitucionais do usuário da internet no Brasil, direitos já apontados na presente obra, e mesmo indevida orientação ao Poder Judiciário (§ 3º), violadora dos dispositivos constitucionais definidores da atuação de referido Poder (arts. 92 a 126 da Carta Magna). (FIORILLO, 2015, p.136).

Embora tenha sido alvo de críticas, especialmente em relação à responsabilização por danos decorrentes de conteúdo gerado por terceiros, o Marco Civil da Internet foi bem aceito pelo público e por especialistas em sua maioria. O físico e cientista da computação, Sir Tim Berners-Lee, considerado um dos criadores da internet da forma como conhecemos hoje, teceu diversos elogios ao Marco Civil da Internet. Em publicação feita no site World Wide Web Foundation no dia 24 de março de 2014, ele elogiou a Lei n. 12.965, de 23 de abril de 2014, nos seguintes termos:

> Se o Marco Civil for aprovado, sem maiores adiamentos ou modificações, este seria possivelmente o melhor presente de aniversário para os usuários de internet do Brasil e do mundo. Eu espero que, aprovando esta lei, o Brasil fixe sua orgulhosa reputação como um líder mundial em democracia e progresso social e ajude a inaugurar uma nova era, uma onde os direitos dos cidadãos em todos os países do mundo são protegidos por leis de direito digitais. (BERNERS-LEE, 2014, n.p)

Teixeira (2021) foi outro especialista que também fez elogios ao Marco Civil da Internet:

> por isso, vemos com bons olhos a promulgação do Marco Civil da Internet na medida em que se trata de uma lei principiológica, mas com a capacidade de promover uma maior transparência e confiança no uso da internet, bem como ampliar a segurança jurídica no Brasil, especialmente a evitar divergências de decisões judiciais no campo da responsabilidade civil de provedores e intermediários e o exercício da liberdade de expressão e a proteção da privacidade dos usuários, produzindo consequentemente bons efeitos para o comércio eletrônico brasileiro. (TEIXEIRA, 2021, p.178)

Foram levantados os principais aspectos do Marco Civil da Internet, com enfoque especial à tutela de direitos fundamentais, notadamente o direito fundamental à privacidade e à proteção de dados pessoais.

Deste modo, passamos então para a análise da Lei nº 13. 709, de 14 de agosto de

2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD).

4.3 Lei Geral de Proteção de Dados

A Lei n. 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD) é sem dúvidas um grande marco na proteção de dados e no direito à privacidade de pessoas físicas, especialmente no meio digital.

Ela está presente no ordenamento jurídico brasileiro desde 14 de agosto de 2018 e tinha previsão para entrar em vigor no prazo de 18 meses. Contudo, sofreu alterações pela Lei n. 13.853/2019 (lei que criou a ANPD – Autoridade Nacional de Proteção de Dados), tendo seu prazo para início de vigência ampliado para dois anos, estando em vigor, dessa forma, desde 16 de agosto de 2020.

É de se destacar que, além de questões jurídicas, a demora para entrada em vigor da LGPD se deve a todas as suas implicações econômicas. Afinal, a utilização de dados pessoais para fins de publicidade das redes é uma das principais responsáveis pelo sucesso de algumas das maiores empresas do mundo, especialmente Amazon, Apple, Facebook e Google, conhecidos como os ‘’Big Four’’ da tecnologia.

Todas essas grandes corporações, e muitas outras, trabalham com algoritmos capazes de entender o comportamento dos usuários e, a partir disso, enviar anúncios direcionados e específicos para eles.

De acordo com Laura Schertel Mendes (2014), no século XX a economia era majoritariamente baseada na produção em massa, com bens padronizados, em grande quantidade e por baixo custo. No entanto, nessas primeiras décadas do século XXI vêm sendo observada uma mudança desse modelo para um marketing segmentado, com mercados investindo em produtos customizados, singulares e pautados na alta qualificação do mercado consumidor.

Desse modo, atualmente, temos a chamada publicidade comportamental, também conhecida por *behavior advertising*, justamente pelo fato de as empresas, especialmente no mercado digital, buscarem anúncios personalizados com base nos dados e comportamentos dos usuários da internet. Essa prática é possibilitada pela técnica *data mining*, ou mineração de dados, entendida por Laura Schertel Mendes nos seguintes termos:

> Data mining, ou mineração de dados, é o processo pelo qual dados de difícil compreensão são transformados em informações úteis e valiosas para a empresa, por meio de técnica informática de combinação de dados e de estatística. Isso significa

> que, por meio de uma única tecla, empresas são capazes de unir e combinar dados primitivos de uma pessoa, formando novos elementos informativos. (MENDES, 2014, p.204)

Assim, o indivíduo no mundo digital é formado por dados, que formam um perfil a seu respeito. Com base em uma análise desse perfil, é possível entender suas decisões e traçar o seu perfil de consumidor, de modo a mostrar para ele majoritariamente anúncios personalizados e relevantes, aumentando o lucro das empresas envolvidas.

Bruno Ricardo Bioni (2018) aduz que esse modelo explica o porquê da ampla maioria dos conteúdos da internet ser ‘’gratuita**’** , destoando do padrão de consumo tradicional, no qual um produto ou serviço é oferecido em troca de uma prestação pecuniária.

Nos dizeres da especialista Patrícia Peck Pinheiro “Há uma expressão atual para retratar o modelo de riqueza da web que diz: se o serviço for gratuito, você não é o freguês, você é produto!” (PINHEIRO, 2013, p.91).

Assim, nesse modelo, o produto é o usuário, enquanto a contraprestação é o fornecimento de seus dados. Dito de outro modo, você ‘’paga’’ o Facebook, por exemplo, informando sua data de nascimento, seu CEP, compartilhando sua localização ou simplesmente interagindo na rede social.

O sucesso econômico dessa estratégia é absolutamente evidente para as empresas. De acordo com ranking feito pela Kantar Brandz e publicado no site G1, a Apple é a empresa mais valiosa do mundo em 2022, sendo estimada em US$ 947,062 bilhões. O Google vem logo em seguida, com US$ 819,573 bilhões. Já em terceiro lugar vem a poderosa Amazon, valendo US$ 705,646 bilhões.

Contudo, se para essas empresas tecnológicas o sucesso é claro, para o público isso nem sempre ocorre. Embora não seja o foco do presente trabalho, é inegável que esse modelo é alvo de severas críticas por alguns especialistas.

Muitas vezes, os dados dos usuários são utilizados como parâmetros questionáveis pelas empresas. Nos Estados Unidos, por exemplo, é comum bancos e outras instituições financeiras utilizarem o CEP das pessoas para dar sua nota em escores de crédito. Ocorre que pessoas que moram em endereços mais humildes – onde o número de inadimplentes é maior -, têm seu escore abaixado, mesmo que honre com todas as suas dívidas.

A autora Cathy O’Neil, no livro ‘’Algoritmos de Destruição em Massa’’ explica muito bem a situação:

> Hoje somos somados de todas as formas possíveis conforme estatísticos e matemáticos organizam como puderem uma salada de dados, de nossos CEPs e padrões de navegação na Internet a nossas compras recentes. Muitos de seus modelos

> pseudocientíficos tentam estimar nossa credibilidade, dando a cada um de nós assim chamados e-escores. (O'NEIL, 2021, p. 134).

Com base nessa lógica, fica muito mais difícil uma pessoa de um bairro humilde conseguir um bom empréstimo perante instituições financeiras apenas porque mora em um bairro com pessoas que pagam menos. Ora, os bancos deveriam se importar apenas com o comportamento que determinado indivíduo teve no passado, e não com a forma pela qual pessoas parecidas com ele se comportaram.

Com esse modelo fica muito mais difícil, por exemplo, um jovem de origem humilde conseguir um empréstimo bom e justo para investir em seu próprio negócio. Além de todas as dificuldades, ele teria que ‘’carregar nas costas’’ o peso de ter nascido naquele determinado local. Não é difícil de imaginar, portanto, que essa forma de tratamento realizada por algumas instituições tende a aumentar ainda mais a desigualdade social e a marginalização de pessoas com menor poder aquisitivo.

Indo mais além, nos Estados Unidos descobriu-se que empresas de seguro para carros também utilizavam o escore de crédito dos clientes como parâmetro para a cotação. Ou seja, em vez de serem julgados pela sua qualidade na direção, os motoristas eram avaliados com base em seus compromissos financeiros. Cathy O'Neil analisou a situação da seguinte forma:

> Mas o Consumer Reports descobriu que os e-escores, que incluem todo o tipo de dados demográficos, muitas vezes valem mais do que o histórico do motorista. Em outras palavras, o modo como você administra dinheiro pode importar mais do que como dirige o carro. No estado de Nova Iorque, por exemplo, uma queda na classificação de crédito de um motorista de "excelente" para apenas "bom" poderia elevar o custo anual do seguro em US$ 255. E, na Flórida, adultos com históricos limpos de direção e baixos escores de crédito pagam em média US$ 1.552 a mais do que os mesmos motoristas com escores excelentes e com uma condenação por dirigir embriagado. (O'NEIL, 2021, p. 154).

Além da utilização dos dados das pessoas para critérios questionáveis, é de se destacar também que esse modelo de algoritmos baseados no comportamento também fere o direito de acesso à informação do usuário. Ocorre que, ao ser mostrado para ele apenas o que está de acordo com o perfil criado para o titular, ele passa a não ser mais exposto a conteúdos que não estejam encaixados nesse perfil.

Dito de outro modo, é como se o comportamento o usuário na internet criasse uma bolha para ele, de modo que seja muito difícil para ele receber conteúdos mais gerais e fora daquele nicho. Além de poder gerar um isolamento social, esse modelo pode deixar o usuário alienado e ‘’preso’’ a aquilo que o algoritmo entende que é relevante para ele.

Deste modo, com todas essas questões envolvendo os dados dos usuários é que foi elaborada a Lei Geral de Proteção de Dados, de modo a regulamentar os direitos do titular dos

dados, o compromisso e as responsabilidades das empresas que trabalham com os dados dos usuários, além de estabelecer diretrizes para determinar como sites e redes sociais devem apresentar sua política de privacidade.

4.3.1 O que é a LGPD?

Adentrando sobre a LGPD em si, temos que a Lei n. 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD) objetiva, em síntese, dispor sobre o tratamento dos dados pessoais, especialmente nos meios digitais, de modo a proteger os direitos fundamentais da privacidade, liberdade e desenvolvimento da personalidade da pessoa natural.

Dito de outro modo, podemos afirmar que a LGPD cuida da proteção aos dados coletados e armazenados, almejando proteger a privacidade dos brasileiros ou estrangeiros que se encontrem no Brasil. Ela tem como principal foco encontrar um meio entre a liberdade das empresas de utilizar os dados dos indivíduos e uma forma de garantir que as pessoas tenham o seu direito à privacidade e à proteção de dados respeitado.

Ela também busca, de maneira geral, garantir maior transparência e servir como um norte para que as empresas adequem suas políticas de privacidade e deixem os usuários mais cientes de como seus dados podem ser coletados e usados por essas corporações para fins comerciais.

Em síntese, a LGPD foi uma resposta do ordenamento jurídico brasileiro a uma nova necessidade da sociedade: de ter uma lei capaz de expressar de modo simples e objetivo como as empresas podem coletar e processar os dados das pessoas.

Como veremos mais adiante no presente trabalho, a LGPD sofreu grande influência da General Data Protection Regulation (GDPR), que é o regulamento do direito europeu que trata da privacidade e da proteção dos dados pessoais, aplicável em toda a União Europeia e Espaço Econômico Europeu.

4.3.2 Disposições preliminares da LGPD

A LGPD logo no seu art. 2º já traz os seus fundamentos. No inciso I temos o ‘’respeito à privacidade’’ (BRASIL, 2018) e no inciso IV observamos a ‘’inviolabilidade da intimidade, da honra e da imagem’’ (BRASIL, 2018). Com isso, já observamos de forma clara o intuito do legislador de proteger os indivíduos e garantir sua honra, imagem e privacidade.

No inciso V vemos ‘’o desenvolvimento econômico e tecnológico e a inovação’’(BRASIL, 2018). Neste dispositivo, fica perceptível que a LGPD não se opõe fielmente às políticas adotadas pelas empresas, apenas está buscando proteger os usuários de determinados abusos que essas políticas podem causar. O inciso VI é bastante interessante ao garantir ‘’a livre iniciativa, a livre concorrência e a defesa do consumidor’’(BRASIL, 2018). Nesse caso, vemos que no mesmo dispositivo está assegurado o direito à livre iniciativa e livre concorrência, mas sem esquecer que os direitos dos consumidores também precisam ser assegurados.

O art. 5º, por sua vez, é bastante relevante ao trazer diversos conceitos, dentre os quais destaca-se os tipos de dados, quem é o titular e quem são o controlador e o operador, nos seguintes termos:

> 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;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (BRASIL, 2018).

Dentro desse contexto, destaca-se que apenas os dados pessoais de pessoas naturais serão protegidos por essa lei.

Além do mais, é relevante abordar sobre a diferença entre o dado pessoal e o dado pessoal sensível. O primeiro é o dado em sentido amplo, compreendido como uma informação relacionada a uma pessoa natural. O segundo, por sua vez, é mais específico, sendo uma informação ligada a um assunto mais polêmico e controvertido, como religião, política ou sexualidade. Dessa forma, a violação a um dado sensível certamente causa maiores transtornos ao indivíduo lesado, justamente por dizer respeito a um tema íntimo de sua personalidade.

Imprescindível citar também a ideia de ‘’tratamento’’, conceituado pela Lei Geral de Proteção de Dados nos seguintes termos:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação,

> avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (BRASIL, 2018)

Assim, ‘’tratamento’’ foi o termo utilizado pela legislação para definir um procedimento relacionado ao uso do dado pessoal de um indivíduo. Patrícia Peck Pinheiro entende o conceito de tratamento da seguinte forma:

> Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (PINHEIRO, 2021, p.47).

Destaca-se também que todas essas hipóteses previstas no dispositivo constituem apenas um rol exemplificativo. Dessa forma, outras hipóteses, não previstas na Lei n. 13.709/2018, também poderão ser consideradas tratamento de dados. Tarcísio Teixeira corrobora com esse pensamento:

> Como se pode perceber, embora o conceito legal traga inúmeras hipóteses (coleta, recepção, arquivamento etc.), trata-se de um rol exemplificativo ao expressar que “toda operação realizada com dados pessoais, como (...)”. Isto é, pode haver outras hipóteses não previstas pela lei relacionadas com dados pessoais que serão tidas por tratamento de dados, logo, sujeita à Lei n. 13.709/2018. (TEIXEIRA, 2021, p.397)

Outrossim, é fundamental destacarmos desde já o conceito de consentimento, expresso no inciso XII do art. 5º da LGPD:

> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (BRASIL, 2018)

Nesse sentido, entendemos que o consentimento deve ser, acima de tudo, válido. E a LGPD estabelece critérios para que esse consentimento tenha validade, qual seja o principal, o caráter livre, informado e inequívoco, que será melhor trabalhado mais adiante neste presente trabalho.

Mas desde já, relevante citar que a ideia de consentimento constitui um eixo central para a Lei Geral de Proteção de Dados, que emponderou ao titular o direito ter seus dados tratados pelo controlador e operador apenas se ele quiser e consentir de tal modo.

Vendo sob a perspectiva contrária, as empresas e corporações precisam do consentimento do usuário para que possam, por exemplo, coletar, classificar e utilizar os seus dados.

Assim, observamos como o consentimento do titular é determinante para o processo de utilização dos seus dados, constituindo essa uma das grandes premissas da Lei Geral de

Proteção de Dados.

4.3.3 Pontos de Convergência e Divergência entre a LGPD e a GDPR

Como vimos mais acima no presente trabalho, a Lei Geral de Proteção de Dados teve como grande fonte de inspiração a *General Data Protection Regulation* (GDPR), que é o regulamento europeu sobre a proteção de dados.

Desse modo, justamente por a GDPR ser a ‘’mãe’’ da LGPD, as duas leis são bastante parecidas, possuindo diversos pontos de similitude. O primeiro deles, e mais óbvio, diz respeito ao objetivo, pois ambas possuem o mesmo propósito: estabelecer princípios e diretrizes sobre coleta e tratamento de dados, de modo a garantir o desenvolvimento econômico, mas sem deixar de lado o respeito à privacidade, liberdade e proteção de dados dos indivíduos. Patrícia Peck Pinheiro aborda a questão nos seguintes termos:

> Considerando a comparação entre a LGPD e o GDPR, ambas as legislações têm como objetivo o regramento do tratamento de dados pessoais, buscando em si a defesa dos direitos fundamentais das pessoas naturais. (PINHEIRO, 2021, p.86)

Outro ponto em comum é o conceito de dado pessoal, entendido como qualquer informação de pessoa natural identificada ou identificável. Assim, estão excluídas as pessoas jurídicas e os dados anônimos, desde que o processo de anonimização possa ser revertido.

Nas duas leis os dados anônimos são compreendidos como aqueles que não se relacionam a uma pessoa natural identificada ou identificável. Além do mais, na GDPR também há a conceituação de dado sensível. No regulamento europeu, entretanto, ele recebe o nome de dado especial, mas é equivalente ao dado sensível da LGPD. Assim, os dados sensíveis, ou especiais, são aqueles relacionados a opiniões políticas, crenças religiosas, dados genéticos e relativos à saúde, à vida ou orientação sexual, assim como acerca de crenças filosóficas ou ligados a origem racial.

Outro ponto de convergência entre as duas leis é acerca dos direitos dos titulares. Por exemplo, tanto na LGPD quanto no GDPR o titular pode se opor ao tratamento dos seus dados. Assim, o consentimento é a pedra basilar das duas leis.

Além disso, as duas leis exigem que os responsáveis pelo tratamento informem com precisão e de forma detalhada de que modo seus dados serão tratados, o que representa uma grande conformidade ao princípio da transparência.

Outrossim, na LGPD e na GDPR o titular pode solicitar a exclusão de seus dados pessoais. As exceções a essa regra também são muito parecidas, que ocorrem nos casos de dados

utilizados com objetivos artísticos, acadêmicos, jornalísticos ou de pesquisa.

Superadas as semelhanças entre a LGPD e a GDPR, sem pretensão de esgotar o assunto, até por não ser o foco do presente trabalho, vamos analisar as principais diferenças entre as duas leis.

Deve-se destacar, antes de tudo, que a LGPD é uma lei mais curta e resumida, se comparada com a GDPR. Logo, em muitos casos, as maiores divergências entre as leis não se dão por um conflito entre ambas, mas sim por alguma previsão da GDPR não constar no texto da LGPD.

Como um exemplo disso, temos que, de acordo com a GDPR, quando for constatado pelo relatório de impacto um alto risco, caso não sejam tomadas medidas para mitigar tal risco, o responsável pelo tratamento dos dados deve comunicar a autoridade nacional antes de realizar o tratamento dos dados. Todavia, a LGPD não traz essa necessidade de consulta prévia à Agência Nacional de Proteção de Dados (ANPD), embora não haja nenhum impeditivo de que essa consulta possa ser feita.

Relevante citar também que a GDPR traz que o regulamento europeu se aplica à proteção de dados pessoais de pessoa natural independentemente da nacionalidade. A LGPD, por sua vez, não traz nenhuma previsão nesse sentido. Entretanto, importante frisar que a LGPD, assim como todas as leis infraconstitucionais, deve ser interpretada conforme a Constituição. E com base nos princípios norteadores do texto constitucional e na jurisprudência firme do STF, os direitos fundamentais do art. 5º da Constituição Federal se aplicam aos estrangeiros, mesmo aqueles não residentes. Logo, o direito fundamental à proteção de dados, expresso no inciso LXXIX do art. 5º, segue esta toada. Dessa forma, natural de se concluir que a Lei Geral de Proteção de Dados também se aplica aos estrangeiros, mesmo sem haver nenhuma previsão expressa nesse sentido.

Acerca do tratamento de dados de crianças e adolescentes, a LGPD afirma que os menores de 18 anos precisam do consentimento de pelo menos um de seus pais ou responsáveis para o tratamento dos seus dados. Na RGPD, por outro lado, pessoas com 16 anos ou mais já são consideradas aptas a dar o seu próprio consentimento.

Outra diferença significativa entre as leis é que o regulamento europeu não traz nenhuma previsão acerca da utilização dos dados pessoais para ajudar nos estudos sobre a saúde pública. Essa possibilidade, no entanto, está prevista na LGPD, a qual afirma que entidades podem fazer uso desses dados, desde que dentro da entidade, em um ambiente estritamente controlado, objetivando realizar estudos para a saúde pública e adotando, sempre que possível, a anonimização ou a pseudonimização dos dados.

No que tange à violação ou vazamento dos dados, a GDPR traz que a notificação dos fatos às autoridades competentes deve ocorrer no prazo de até 72 horas. No entanto, a lei brasileira apenas afirma que, no caso de violação das informações dos indivíduos, o controlador comunicará à autoridade nacional em prazo razoável. Esse prazo subjetivo abre margem para que a ANPD, que é a autoridade brasileira, só fique ciente do incidente muito tempo depois, o que pode dificultar a reparação dos danos sobre as informações do titular.

Acerca da relação entre controlador e operador de dados, destaca-se que a GDPR impõe a exigência de um contrato entre ambos, de modo a explicitar o tratamento dos dados. A LGPD, por sua vez, afirma apenas que o operador realizará o tratamento dos dados sob orientação do controlador, mas sem exigir qualquer contrato.

Em síntese, a RGPD e a LGPD são leis muito semelhantes, seja por versarem sobre o mesmo tema e terem o mesmo propósito, seja porque a lei brasileira se inspirou bastante no regulamento europeu. As diferenças entre ambas são pontuais e se referem a aspectos específicos. Mas de forma geral, a GDPR é uma lei maior, mais detalhada e mais restritiva se comparada à LGPD, com regras mais determinadas, deixando menos discricionariedade para os agentes envolvidos e garantindo uma proteção maior aos direitos fundamentais dos usuários.

4.3.4 O que é um dado pessoal?

Antes de destrincharmos mais ainda a LGPD, faz-se necessário destacar mais precisamente o que de fato é um dado pessoal, vez que tal conceito é motivo de questionamentos.

Destaca-se que, em sentido mais amplo, o dado pessoal é uma informação ligada a uma pessoa natural, identificada ou identificável. Assim, é algo que pode identificar uma pessoa, como seu nome completo, o número do seu CPF, o número do RG, a data de nascimento ou seu endereço.

Com base nisso Tarcísio Teixeira fez a seguinte divisão:

> Assim, os dados pessoais poderiam ser classificados em diretos e indiretos: diretos quando as informações identifiquem diretamente a pessoa e indiretos quando a pessoa puder ser identificada pelas informações. (TEIXEIRA, 2021, p.397)

Relevante salientar que, como os dados pessoais compreendem as informações que identificam ou poder identificar um indivíduo, os dados anonimizados não são considerados dados pessoais para fins de LGPD, pois eles são considerados dados relativos a titular que não possa ser identificado. O art. 12 é claro a esse respeito:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. (BRASIL, 2018).

Além disso, é de se destacar também o processo de anonimização, que consiste na utilização de meios técnicos e razoáveis para que um dado perca a capacidade de associação, direta ou indireta, a um indivíduo.

Os dados anonimizados são diferentes dos dados pseudonimizados, pois esses últimos ainda podem ser associados a um indivíduo por conta de um elemento de ligação que fica registrado separadamente em um ambiente controlado e seguro.

Outrossim, dada a importância da conceituação, frisa-se novamente a diferenciação entre dados pessoais e dados sensíveis. Os primeiros nada mais são do que gêneros do segundo. Logo, os dados sensíveis também são informações relacionadas a um titular, mas que versam 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" (LGPD, art. 5º, II).

O especialista Tarcísio Teixeira (2021) ainda destaca que até mesmo a íris dos olhos e a impressão digital nos dedos são exemplos de dados sensíveis, justamente por conta de seu caráter mais íntimo. Ele também é pontual ao destacar a diferenciação entre esses dois tipos de dados "A título distintivo e ilustrativo, enquanto o dado pessoal está relacionado à privacidade do titular, o dado pessoal sensível diz respeito à intimidade dele." (TEIXEIRA, 2021, p.400).

Feita essa maior explanação sobre a conceituação e a diferenciação dos dados pessoais, vamos a uma análise sobre a aplicabilidade da Lei Geral de Proteção de Dados.

4.3.5 Aplicabilidade da LGPD

A Lei n. 13.709/2018 se aplica a relações jurídicas estabelecidas tanto no meio físico quanto no meio digital, alcançando a todos que realizem tratamento de dados, sejam pessoas físicas, sejam pessoas jurídicas, desde que a operação de tratamento satisfaça pelo menos um dos requisitos: (1) ocorra em território nacional; (2) possua por objetivo a oferta ou o fornecimento de bens, serviços ou tratamento de dados de pessoas localizadas no território nacional ou (3) os dados tenham sido coletados no território nacional.

Dessa forma, não há nenhum óbice para a aplicação da LGPD a empresas estrangeiras, desde que elas satisfaçam pelo menos um dos requisitos acima destacados.

Por exemplo, o Facebook e o Google são pessoas jurídicas norte-americanas, mas

que coletam os dados de diversos indivíduos brasileiros no território nacional. Logo, elas precisam realizar o tratamento desses dados conforme as diretrizes impostas pela LGPD.

O art. 4º, por seu turno, traz alguns casos em que a LGPD não será aplicada. Veja-se abaixo:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. […] (BRASIL, 2018)

Dessa forma, constatamos que o legislador buscou, na balança entre direito à privacidade e segurança nacional, pender para o lado coletivo, de modo que os indivíduos tenham seus direitos respeitados, mas até o limite deles ameaçarem a segurança pública, a defesa nacional, a segurança do estado ou as atividades de investigação e repressão das infrações penais.

Além do mais, observamos, pela leitura dos incisos I e II, que a preocupação do legislador está mais relacionada com a utilização dos dados para fins comerciais. Sendo assim, a LGPD não se aplica quando os fins são exclusivamente artísticos, jornalísticos ou acadêmicos, ou quando feito por pessoas naturais com objetivos particulares e não econômicos.

Desse modo, o principal âmbito de incidência da Lei Geral de Proteção de Dados é justamente proteger o titular que oferece os seus dados em troca do acesso aos conteúdos da internet. Isso não é surpresa, pois mais acima vimos que a pressão maior para uma lei que regulasse os dados no Brasil girava em torno de uma necessidade causada pela publicidade comportamental, em que as empresas utilizam cada vez mais o usuário da internet como o produto, na medida em que seus dados são a principal forma de pagamento. Patrícia Peck Pinheiro analisa muito bem a situação:

> Como visto, a necessidade de uma lei específica sobre proteção dos dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências. (PINHEIRO, 2021, p.54)

Feita essa análise sobre a aplicabilidade da LGPD, vamos partir para o tratamento dos dados.

4.3.6 Tratamento dos dados pessoais

O tratamento de dados é o cerne da LGPD. Ou seja, não se pode falar sobre a Lei 13.709/2018 sem abordar como o ocorre o tratamento dos dados pessoais dos indivíduos.

O art. 6º da Lei Geral de Proteção de Dados indica uma série de princípios que precisam ser respeitados para que os direitos fundamentais das pessoas envolvidas sejam respeitados. Para uma melhor compreensão sobre esse importante dispositivo, a tabela abaixo contempla os princípios:

Tabela 1: princípios do art. 6º da Lei Geral de Proteção de Dados

Princípios	Conceituação
Finalidade	Os dados coletados devem ter um fim específico, claro e informado ao titular, devendo o tratamento se ater fielmente a essa finalidade.
Adequação	O tratamento deve ser compatível com as finalidades informadas ao titular, sempre adequadas ao que o titular de fato consentiu.
Necessidade	O tratamento dos dados deve ser o mínimo necessário para que a finalidade seja atendida, não podendo haver excessos.
Livre Acesso	Os titulares devem ter um acesso fácil e gratuito sobre os seus dados coletados, a forma e a duração do tratamento.
Qualidade dos dados	O tratamento dos dados deve corresponder ao que foi coletado, observando a necessidade, a clareza, a relevância e a atualização dos dados, de modo a cumprir a finalidade do tratamento.
Transparência	Os dados e o tratamento devem ser informados de forma clara, precisa e facilmente acessível, resguardados os segredos comercial e industrial.
Segurança	Medidas técnicas e administrativas devem ser utilizadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.
Prevenção	Medidas devem ser tomadas de modo a prevenir a ocorrência de danos em decorrência do tratamento dos dados pessoais.
Não discriminação	O tratamento não pode ser usado para fins discriminatórios ilícitos ou abusivos.
Responsabilização e Prestação de Contas	O agente deve demostrar que está adotando medidas capazes e eficazes de comprovar a observância e o cumprimento da legislação sobre dados pessoais, assim como, que está buscando a eficácia dessas medidas.

Fonte: elaborado pelo autor.

Aprofundando um pouco mais nos princípios abordados na tabela, observamos que os princípios do livre acesso e da transparência são muito parecidos. Contudo, eles se diferem no sentido em que o princípio do livre acesso busca garantir uma consulta facilitada para o usuário que quer acessar a forma de tratamento dos seus dados, enquanto que o princípio da transparência diz respeito à clareza das informações, isto é, se as informações sobre o tratamento estão claras e condizentes com a realidade.

Além disso, pode haver confusão também entre os princípios da segurança e da prevenção. Embora sejam parecidos, eles se diferem porque o primeiro é mais geral, abrangendo hipóteses de proteção contra erro ou violação no tratamento de dados. O segundo, por sua vez, está mais focado em prevenir a geração de danos significativos aos indivíduos.

Ainda sobre o princípio da segurança, destaca-se que entre os artigos 46 e 49 da LGPD estão expressas previsões para reforçar tal princípio. Dentre eles, destaca-se a responsabilidade dos agentes de tratamento, presente no artigo 47:

> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. (BRASIL, 2018).

Os princípios acima destacados norteiam todo o tratamento dos dados, previsto com mais precisão entre os artigos 7º e 15 da Lei Geral de Proteção de Dados.

O art. 7º, inciso I, traz o principal caso que permitirá o tratamento dos dados: o consentimento fornecido pelo titular. Embora seja um tópico destrinchado mais adiante no presente trabalho, é relevante destacar que ele constitui uma das bases da Lei Geral de Proteção de Dados.

Em suma, entendeu o legislador que a principal forma de garantir o respeito aos direitos fundamentais da privacidade e da proteção de dados é conferindo ao próprio titular o poder de aceitar ou não ter seus dados tratados por determinada empresa ou corporação.

O art. 8º da mesma lei destaca que esse consentimento, para que seja considerado válido, deve ser fornecido por escrito ou por outro meio que comprove a manifestação de vontade do titular. Além do mais, caso seja por escrito, o inciso I do mesmo artigo afirma que ele deverá constar com cláusula destacada das demais cláusulas contratuais.

Neste aspecto, o legislador buscou conferir maior eficácia ao consentimento do titular, de modo que ele não seja vazio e sem validade. Além disso, serve como uma diretriz para as empresas, para que elas sempre destaquem a cláusula do consentimento, tendo em vista que o usuário poderia se confundir e aceitar o tratamento de seus dados sem possuir qualquer intenção disso.

Outrossim, com base no §4 do mesmo artigo, o consentimento deverá estar relacionado a finalidades determinadas, sendo nulas as autorizações genéricas.

Embora o consentimento seja a principal forma de permitir o tratamento de dados, o art. 7º da LGPD ainda traz outras possibilidades, como para cumprir uma obrigação legal ou regulatória, para proteger a vida e a integridade física de titular ou terceiro, para proteger o crédito etc.

Em todos esses casos, a semelhança é que decorrem necessariamente da lei, sendo bases legais que podem, assim como o consentimento do titular, autorizar o tratamento dos dados pessoais.

Além dessas possibilidades, uma outra forma de se permitir o tratamento dos dados pessoais é quando houver o legítimo interesse do controlador. Infelizmente a LGPD não pormenorizou o que de fato é o legítimo interesse, que muitas vezes soa como bastante genérico e abstrato. Tarcísio Teixeira (2021) analisou muito bem a situação:

> A questão do interesse legítimo ou legítimo interesse é uma das questões mais delicadas da LGPD. Mas o que vem a ser legítimo interesse? Vamos por partes. Legítimo quer dizer algo justo, razoável; já interesse significa aquilo que é importante. Desse modo, conceitualmente, pode-se afirmar que o legítimo interesse do controlador é "aquilo que lhe é justo e importante". Convenhamos que se trata de um conceito muito abstrato e aberto (TEIXEIRA, 2021, p.413).

O art. 10 da Lei Geral de Proteção de Dados procura estabelecer alguns limites para o legítimo interesse. Com base no §1, temos que apenas os dados pessoais estritamente necessários para a finalidade podem ser tratados. O §2 aborda que o controlador deve sempre se pautar pela transparência. O §3, por sua vez, traz a interessante possibilidade de a autoridade nacional solicitar um relatório de impacto à proteção de dados pessoais, no caso de tratamento com fundamento no interesse legítimo, desde que respeitados os segredos comercial e industrial.

Mesmo com todas essas medidas para controlar o legítimo interesse do controlador, é inegável que essa hipótese de tratamento de dados é bastante questionável e pode gerar problemas para os direitos fundamentais do titular, tendo em vista que, por exemplo, não é sempre que o relatório de impacto será solicitado pela autoridade nacional. Assim, estamos diante de uma discricionariedade da ANPD, que poderá falhar em sua missão de proteger a privacidade e a proteção de dados dos usuários.

Como os dados pessoais sensíveis são relacionados à intimidade do indivíduo e possuem um maior poder de causar impacto negativo em caso de violação, eles possuem um regime jurídico diferenciado. O art. 11, inciso I, da Lei 13.709/2018 destaca que o consentimento do titular ou responsável legal continua sendo o principal fator para autorizar o

tratamento de dados pessoais sensíveis.

O inciso II deste mesmo dispositivo aborda os casos que autorizam, mesmo sem o consentimento do titular, o tratamento de dados sensíveis:

> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018).

É de se destacar, portanto, que o rol para o tratamento de dados pessoais sensíveis é mais curto do que o de dados pessoais em geral, o que mostra o cuidado do legislador nesse ponto acerca dos cuidados com os direitos dos usuários.

Dentro desse contexto, destaca-se que no rol acima citado não há menção de uso de dados sensíveis para a proteção do crédito, o que é autorizado pela lei no caso de outros dados pessoais, nos termos do art. 7º, inciso X, da LGPD.

Ademais, interessante destacar que o legítimo interesse, autorizado para os dados pessoais, não está presente para os dados sensíveis, justamente para garantir maior proteção à esfera mais íntima da vida dos indivíduos.

Outro dispositivo que merece destaque é o art. 11, §3, da LGPD, no qual aborda que a comunicação e o uso compartilhado de dados sensíveis por controladores para obter vantagem financeira (por exemplo, com anúncios) pode ser objeto de vedação por parte do poder público. Essa restrição é de extrema importância para evitar a comercialização e a mercantilização da vida privada das pessoas.

Assim, existem severas restrições ao uso de anúncios personalizados com base em aspectos potencialmente discriminatórios ou que digam respeito à vida íntima das pessoas. O Google, por exemplo, deixa isso bem claro em sua política de privacidade, ao afirmar que: ‘’Não mostramos anúncios personalizados com base em categorias sensíveis, como raça, religião, orientação sexual ou saúde.’’

Já acerca da proteção de dados de crianças e adolescentes, o art. 14 da LGPD afirma

que ela deverá ser feita com base no melhor interesse desses indivíduos. Destaca-se que, de acordo com o art. 1º da Lei 8.069 (Estatuto da Criança e do Adolescente), considera-se criança a pessoa com até 12 anos incompletos, e adolescente aquela que possui entre 12 e 18 anos de idade.

O parágrafo 1º do art. 14 da LGPD aduz que o tratamento dos dados de crianças e adolescentes deve ocorrer mediante consentimento específico por pelo menos um dos pais ou responsável legal. O §5º complementa afirmando que os controladores deverão realizar todos os esforços razoáveis para verificar que esse consentimento foi realmente dado pelo responsável da criança, observando as tecnologias disponíveis no momento do tratamento.

Relevante citar ainda que o §3º traz uma importante exceção a essa regra ao abordar que os dados de crianças e adolescentes podem ser coletados sem o consentimento dos pais quando a coleta for necessária justamente para contatar os pais. Assim, o legislador foi bastante perspicaz, pois imaginou a possibilidade de o menor estar perdido ou desacompanhado, por exemplo. Contudo, esse dispositivo menciona que nesse caso os dados serão utilizados apenas uma única vez, sem armazenamento, e que não poderão ser repassados a terceiros sem o devido consentimento dos pais ou responsável.

O art. 14, §4, da LGPD também é relevante ao destacar que o controlador não pode condicionar a participação de crianças e adolescentes em jogos e aplicações na internet ao fornecimento de informações pessoais além das totalmente necessárias à atividade. Nesse caso, o legislador também foi bastante preciso, pois coibiu que jogos e aplicações da internet, que têm alto apelo infantil, pudessem se aproveitar disso para coletar muitos dados de crianças e adolescentes.

O término do tratamento dos dados também é um aspecto muito relevante da Lei Geral de Proteção de Dados, pois, se constatada alguma hipótese de término do tratamento, ele deverá imediatamente ser finalizado, sob pena de violação à proteção de dados e à privacidade dos indivíduos.

Dessa forma, podemos afirmar que o limite de atuação é um dos requisitos de validade do tratamento de dados. Nesse sentido, esse procedimento não deve ser realizado por tempo indeterminado. O art. 15 da Lei 13.709/2018 apresenta as seguintes hipóteses de término no tratamento dos dados:

> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse

> público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018).

Feita essa explanação sobre as hipóteses de tratamento, algumas críticas podem ser elaboradas a partir das atuações das empresas e dos sites da internet, que por vezes não estabelecem limites para o tratamento dos dados, agindo como se a finalidade nunca pudesse ser alcançada.

Imaginemos por exemplo a Google, que controla o YouTube, maior plataforma de vídeos do mundo. Dito pela própria Google em sua Política de Privacidade (2022), o histórico de pesquisa do YouTube é levado em consideração para a recomendação de vídeos mais relevantes, de modo a proporcionar uma melhor experiência ao usuário. Explica que isso é necessário para criar um perfil para o titular, com base em sua própria pesquisa.

Acontece que, salvo intensa procura do usuário para interromper esse tratamento, a Google não acaba com ele nunca. Dito de outra forma, a Google nunca para de coletar os dados de pesquisa do titular para a recomendação de vídeos mais interessantes. Assim, perde-se o sentido de um dos principais requisitos para a validade do tratamento dos dados, o seu término, tendo em vista que a Google não pretende terminar com ele nunca, já que ela simplesmente pode alegar que a ‘’finalidade não foi alcançada’’, até porque o perfil do usuário pode mudar.

Em respeito ao que dispõe a Lei Geral de Proteção de Dados em seu artigo 15, a Google deveria possibilitar a criação de um perfil mais personalizado, que alternasse momentos de observância do histórico de pesquisa do indivíduo com outros em que isso simplesmente não seria levado em consideração. Além disso, seria interessante haver uma parte do YouTube destinada a conteúdos mais gerais, desprovidos de personalização.

Contudo, atualmente parece não existir meio-termo para a Google. Assim, ou o histórico de busca do titular será levado em consideração o tempo inteiro e todo o seu perfil do YouTube será elaborado a partir disso, ou então o titular simplesmente bloqueia essa possibilidade e passa a ter um feed muito genérico e totalmente descaracterizado com seus interesses.

Cumpre destacar que, ao término do tratamento dos dados, eles devem ser apagados, conforme dispõe o artigo 16 da Lei Geral de Proteção de Dados:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de

> dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018).

Com base na análise do dispositivo acima referenciado, chegamos à conclusão de que a intenção dos envolvido, inclusive das instituições, é de preservar os dados dos indivíduos, tendo em vista o alto valor de todas essas informações. Contudo, deve-se preponderar em vários casos o direito ao apagamento (direito ao esquecimento). Em último caso, quando houver grande necessidade de continuar com a informação, pode ser aplicada a técnica da anonimização.

4.3.7 Direitos do titular dos dados

Os direitos do titular de dados estão elencados entre os artigos 17 e 22 da LGPD e demonstram uma efetiva preocupação do legislador com os direitos fundamentais dos indivíduos, procurando garantir a liberdade, a intimidade e a privacidade, como dispõe o art. 17 da LGPD.

Além disso, o artigo 18 também é bastante preciso ao afirmar que o titular pode requisitar ao controlador, a qualquer momento, o acesso aos dados; a correção de dados inexatos, desatualizados incompletos; a confirmação da existência do próprio tratamento; a anonimização, bloqueio ou eliminação de dados desnecessários; a revogação do consentimento, entre outras possibilidades.

O art. 19, §3, da LGPD, ainda dispõe que:

> § 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento. (BRASIL, 2018)

Dessa forma, é possível constatar que a Lei Geral de Proteção de Dados realmente tem por grande base a ideia do consentimento, sendo esse o principal gerador da relação envolvida entre o titular e o controlador. Vamos agora analisar a importância do consentimento na LGPD.

5. A IMPORTÂNCIA DO CONSENTIMENTO NA LGPD

Fortemente inspirada no Regulamento Europeu de Proteção de Dados, a LGPD também entende que o consentimento do titular possui um papel de destaque para a ocorrência do tratamento dos dados. Para se ter uma ideia da importância, a palavra ‘’consentimento’’ aparece 35 vezes ao longo da Lei Geral de Proteção de Dados.

O art. 5º, inciso XII, da LGPD, traz o consentimento como sendo a ‘’manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.’’ (BRASIL, 2018). Nesse sentido, o consentimento, para ser classificado como tal, deve atender a alguns critérios específicos.

O aspecto livre do consentimento diz respeito ao controle do usuário acerca do tratamento dos dados. Assim, o titular tem a prerrogativa de escolher quais serão os dados que ele fornecerá para o controlador e quais ele não autoriza o fornecimento, tendo total liberdade nesse sentido.

O caráter informado está relacionado ao titular ter todas as informações necessárias sobre o tratamento, para ponderar se ele de fato consente ou não com os seus dados serem recolhidos e tratados. Nesse caso, todas as informações prestadas pelo controlador devem ser claras, não podendo haver conceitos vagos ou imprecisos.

Por fim, o aspecto inequívoco do consentimento está ligado à ideia de que deve ocorrer uma ação explícita do titular autorizando o uso dos seus dados. Como exemplos disso, podemos destacar o clique na caixa disponibilizada pela empresa ou o clique em um link recebido no e-mail. Dessa forma, não há consentimento por omissão, o consentimento dado pelo usuário deve necessariamente ocorrer por meio de uma ação comissiva.

Além do mais, por ‘’finalidade determinada’’ constatamos que o controlador não pode se utilizar de conceitos vagos, ou seja, o pedido para o tratamento dos dados não deve ocorrer de forma genérica, sem especificações, sob pena de ser considerado nulo, conforme dispõe o art. 8º, §4, da LGPD.

Todos esses requisitos demonstram que o legislador possui um cuidado acerca do consentimento, para que ele não seja uma mera formalidade e de fato expresse uma vontade legítima do titular, sem estar contaminado por qualquer vício, nos termos do art. 8º, §3, da LGPD.

Mais uma evidência acerca do cuidado com o consentimento é encontrada no art. 8º, §1º, da LGPD, o qual dispõe que ‘’caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais’ (BRASIL, 2018). Nesse

caso, o intuito do legislador foi justamente facilitar a identificação do usuário, para que ele não se engane ou fique confuso no momento de consentir.

Outrossim, o titular tem o direito de não querer mais ter seus dados tratados. Sobre isso, o art. 8º, §5, da LGPD, dispõe da seguinte forma:

> § 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. (BRASIL, 2018)

O art. 9º, parágrafos 1º e 2º da Lei Geral de Proteção de Dados busca proteger os reais interesses do usuário nos seguintes termos:

> § 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. (BRASIL, 2018)

Dessa maneira, as informações fornecidas ao titular devem ser claras, transparentes, carentes de qualquer vício ou abuso. De mais a mais, havendo mudanças na finalidade, o controlador deve informar previamente o titular, que terá o poder de discordar das alterações e retirar o seu consentimento.

Feita toda essa análise, podemos identificar como a ideia do consentimento é motivo de muito cuidado pelo legislador. E não é em vão, tendo em vista que o consentimento tem papel de destaque para a ocorrência do tratamento de dados no Brasil.

O art. 2º, inciso II, da LGPD, já deixa isso bastante claro, ao destacar que um dos fundamentos para a proteção de dados é a autodeterminação informativa, que consiste em conferir aos titulares o poder de gerenciar os tratamentos envolvendo seus próprios dados pessoais. Assim, cabe ao próprio titular determinar se seus dados serão coletados e tratados, o que ocorre justamente por sua autorização.

O foco no consentimento não é uma exclusividade da legislação brasileira. Inclusive, desde os anos 70 observa-se o fenômeno da convergência regulatória (*policy convergence*), que consiste em um processo informal, porém coordenado, por meio do qual legislações nacionais foram se moldando em torno de princípios e ideias gerais acerca do tratamento dos dados (BENNET, 1992, p. 111-112 apud MENDES, 2020, p. 512). Esses instrumentos jurídicos foram convergindo em torno da ideia do consentimento.

Assim, a tradição legislativa da proteção de dados tem como foco a questão do consentimento, que serve como mecanismo de legitimação para que ocorra o tratamento dos dados. Portanto, podemos constatar a existência do protagonismo dessa autorização, sendo o grande núcleo legitimador da proteção de dados, o que coloca o indivíduo no centro do ordenamento, pois a ocorrência do tratamento depende de seu aceite.

Sendo assim, inegável reconhecer o mérito dessa convergência regulatória em torno do consentimento, pois estimula os indivíduos a pensarem por conta própria se desejam ou não terem seus dados tratados, além de o colocarem no centro da ideia de autodeterminação informativa.

Contudo, é necessário também pontuar as limitações dessa política, que possui inegáveis adversidades, visto que, por si só, a autorização não se mostra suficiente para proteger efetivamente o direito à privacidade e o direito à proteção de dados dos usuários. A seguir vamos abordar alguns problemas do consentimento.

6. AS LIMITAÇÕES DO CONSENTIMENTO

Como vimos no tópico anterior, a LGPD trata do consentimento com muito cuidado, colocando-o como ponto central para a política de proteção de dados. E, embora essa estratégia tenha muitos benefícios e vantagens, ela também apresenta relevantes insuficiências, que serão melhor trabalhadas a partir de agora.

6.1. Dificuldade de leitura das Políticas de Privacidade no ambiente online

A primeira dificuldade a ser enfrentada por esse método focado excessivamente no consentimento diz respeito às limitações que o próprio usuário pode vir a ter no ambiente online. Ocorre que é de entendimento comum que o indivíduo queira acessar sites para interagir com amigos, realizar pesquisas acadêmicas, ver notícias etc. Paralelo a isso, o meio digital é muito intenso e dinâmico. Logo, acaba por ser muito difícil o usuário parar sua atividade online, deixar seus interesses em segundo plano e ler efetivamente as políticas de privacidade de cada site ou rede social que ele acessa.

Dentro desse contexto, diversas pesquisas pelo mundo comprovam que grande parte dos usuários simplesmente não leem as políticas de privacidade, ou seja, eles adotam o ‘’não li e aceito’’. Uma pesquisa conduzida pela *Pew Research Center* em 2019 constatou que apenas 22% dos americanos leem sempre ou frequentemente as políticas de privacidade, ao passo que 36% confessaram que nunca leem tais políticas.

No Reino Unido as pesquisas também não são animadoras. O site *Thinkmoney* publicou em 2020 uma pesquisa feita pela *The European Commission* em 2016 a qual constatou que 90% dos britânicos aceitam os termos de uso sem compreenderem totalmente o que eles estão aceitando.

No Brasil a realidade não é muito diferente. Uma pesquisa conduzida pela NordVPN em 2021 e publicada no site CanalTech verificou que apenas 38,3% dos brasileiros leem os termos de uso de serviços online e softwares.

Destarte, a velocidade e o dinamismo do ambiente online são por vezes incompatíveis com a leitura concentrada e efetiva de todas essas políticas de privacidade, até porque muitas delas possuem uma linguagem excessivamente técnica e de difícil compreensão para leigos. Não se trata de depreciar o entendimento cognitivo dos usuários, mas sim de reconhecer que as informações exibidas envolvem conceitos técnicos e jurídicos que grande parte das pessoas não estão familiarizadas.

Além do mais, com a quantidade avassaladora de sites presentes na internet, um usuário médio que navega na rede mundial de computadores não tem condições temporais de realizar a leitura de todo o conteúdo das políticas de privacidade. O site *Thinkmoney*, em 2020, fez um levantamento e identificou que leva 17 horas para um usuário médio ler os termos de serviço dos 13 aplicativos mais usados do Reino Unido.

Outras pesquisas sobre o tema já foram realizadas e os resultados não são animadores. Em 2008, Aleecia M. Mcdonald e Lorrie Faith Connor, pesquisadores da *Carnegie Mellon University*, chegaram à conclusão de que, à época, já eram necessárias cerca de 201 horas por ano para que um norte-americano médio conseguisse ler as políticas de privacidade dos sites que ele acessa na internet.

Assim, com todas essas dificuldades, a realidade é que atualmente a maioria das pessoas não conseguem ler efetivamente as políticas de privacidade. Dito isso, como seria possível que elas conferissem um consentimento realmente válido? Desse modo, todos esses obstáculos indubitavelmente enfraquecem o poder do consentimento e da autodeterminação informativa.

6.2. Estratégias do agente de tratamento para obter o consentimento

Outro ponto que afeta consideravelmente o poder do consentimento diz respeito às tentativas e estratégias que os agentes de tratamento utilizam para obter a autorização do usuário. Ora, é inegável que na relação entre agente de tratamento e titular o primeiro tentará utilizar de todas as formas possíveis para obter o aceite do segundo.

Dentre essas estratégias para convencer o usuário a dar o consentimento, está a utilização de termos que soam de forma agradável e benéfica. Um dos mais famosos é a palavra ‘’experiência’ , usada várias vezes quando os sites buscam obter o consentimento do usuário ou então quando eles apenas informam sobre a existência da política de privacidade. Por exemplo, ao acessarmos o portal de notícias R7, em 2022, nos deparamos com a mensagem: ‘’ Utilizamos cookies e tecnologia para aprimorar sua experiência de navegação de acordo com o Aviso de Privacidade.’’

Desse modo, é interessante perceber como a frase ‘’aprimorar sua experiência de navegação’’ soa de forma agradável para o usuário, de modo que passa a ser bem mais difícil ele recusar a política de privacidade do site.

Outros exemplos de táticas para conseguir a aprovação do público são vistas em diversas políticas de privacidade. Como exemplo, podemos citar o site da empresa argentina

Mercado Livre, que em sua política de privacidade, com última alteração ocorrida em julho de 2020, afirma que ‘’Usamos seus dados para criar ferramentas que facilitam o seu dia a dia. Explicaremos aqui o que fazemos com os seus dados.’’

Na política de privacidade do Google também identificamos uma clara tentativa de convencimento do usuário, que ocorre nos seguintes termos:

> Coletamos informações para fornecer serviços melhores a todos os nossos usuários, o que inclui descobrir coisas básicas, como o idioma que você fala, até coisas mais complexas, como anúncios que você pode considerar mais úteis, as pessoas on-line que são mais importantes para você ou os vídeos do YouTube de que você poderá gostar. (GOOGLE, 2022)

No Facebook, observamos tentativas da empresa de Mark Zuckerberg de convencer o titular de que o compartilhamento de informações pessoais entre as empresas da Meta é benéfico para o usuário:

> Para proporcionar uma experiência inovadora que seja integrada, consistente e mais rica em todos os Produtos das Empresas da Meta a fim de permitir interações entre aplicativos, compartilhamento, visualização e engajamento com conteúdo (incluindo publicações e vídeos). (FACEBOOK, 2022).

Dessa forma, podemos ver claramente empresas com lucros exponenciais às custas dos dados dos usuários utilizando uma linguagem tendenciosa, com o objetivo de conseguir o consentimento do titular. O foco de todas essas corporações é tentar convencer o potencial consumidor de que, ao aceitar os termos de uso e a política de privacidade ele estará fazendo a melhor opção para si mesmo, pois assim ele terá uma ‘’melhor experiência**’** . Assim, a intenção muitas vezes não é apresentar de forma fria e racional como seus dados serão tratados e sua atividade será ostensivamente monitorada, mas sim de que toda essa política de dados possibilita que a empresa forneça o melhor tratamento possível para o público.

Destarte, embora seja possível observar que as empresas estejam formalmente se adequando à Lei Geral de Proteção de Dados, elas ainda se utilizam dessa linguagem agradável e tendenciosa para convencer o usuário de que aquilo é o melhor para ele. Não estamos diante de uma proposta imparcial, na verdade, trata-se apenas de uma constante persuasão que, ocorrendo dessa forma, tenderá a ser sempre bem-sucedida. Assim, dificilmente o usuário vai rejeitar os termos de uso e de privacidade do agente de tratamento.

Nesse sentido, estamos diante de uma limitação ao consentimento, pois o titular até tem o poder de rejeitar o tratamento de seus dados, mas a tentativa constante de convencimento do agente de tratamento desequilibra a decisão quase sempre em prol da empresa.

6.3. Assimetria de poderes na relação entre titular dos dados e agentes de tratamento

Outro aspecto que compromete a efetividade do consentimento é a clara assimetria de poderes envolvendo o usuário e o agente de tratamento. Em um contexto no qual o consentimento é visto como o grande legitimador da proteção de dados, é difícil cravar de forma segura que a decisão do usuário é realmente livre, tendo em vista a grande diferença de poder entre as partes envolvidas.

Desse modo, o usuário pode se sentir obrigado a concordar com a política de privacidade da empresa, pois necessita utilizar o serviço, ou então o seu não uso gera consequências desagradáveis para o titular. Assim, vemos que o usuário se encontra em condição de vulnerabilidade. Em alguns casos, ele pode se deparar com sites que ainda utilizam a estratégia do ‘*’take it or leave it’’*, ou seja, ou o titular aceita integralmente os termos de uso e a política de privacidade, ou então ele não conseguirá acessar o conteúdo do site.

Nesse sentido, mesmo não concordando com a política do site, o indivíduo se sente pressionado a aceitá-la, pois em caso contrário pode sofrer um isolamento social, a perda de conteúdos importantes para o seu desenvolvimento acadêmico, a possibilidade de assistir jogos de futebol, ouvir música e ver filmes etc. Dessa maneira, com tanto desequilíbrio de forças, por vezes não há consentimento, e sim obediência. O consentimento acaba por ser protocolar, uma mera formalidade, sem representar qualquer adequação ao princípio da autodeterminação informativa. Laura Schertel Mendes (2020) analisou muito bem a situação:

> Nessas situações, a decisão individual de consentir não é livre e autônoma ou oriunda da avaliação dos ônus e dos bônus envolvidos. Ao revés, ela se origina de uma verdadeira imposição estabelecida por terceiro: consentir ou simplesmente não desfrutar de serviço/produto, que, muitas vezes, sob a perspectiva do indivíduo, é essencial para a sua sociabilidade ou acesso à informação na era digital. (MENDES, 2020, p. 516)

Analisada outra relevante mitigação do consentimento, vamos destrinchar como o desenvolvimento do Big Data também pode comprometer a eficácia da política atual de proteção de dados.

6.4. Desenvolvimento do *big data* e dificuldade de gerenciamento de dados

O desenvolvimento tecnológico possibilitou alterações significativas na forma como os dados dos indivíduos são tratados. Nesse contexto, houve o surgimento da Big Data, que consiste em um termo da tecnologia da informação para representar enormes conjuntos de

dados que podem ser tratados e, a partir disso, gerarem informações relevantes para as empresas que realizam o seu tratamento.

Dessa forma, embora não haja um conceito totalmente solidificado acerca do que de fato é o Big Data, podemos compreendê-lo como um grande conjunto de dados, volumoso, complexo e variável, que pode ser processado por softwares modernos e ajudar no funcionamento das empresas, para que elas produzam produtos cada vez mais eficientes. Ocorre que, com a utilização de redes sociais e plataformas como Google, por exemplo, as pessoas deixam rastros, que nada mais são do que dados, que por fim compõem um grande banco de dados denominado Big Data.

Como muitas vezes esses dados estão espalhados e desconectados, eles não tinham tanta utilidade. No entanto, com o desenvolvimento tecnológico e com o aumento do número de dados na internet, atualmente as empresas estão conseguindo aplicar técnicas modernas e utilizar tais dados para gerar informações úteis e coerentes, que passam a nortear o funcionando dessas grandes corporações, aumentando a produtividade e consequentemente os seus lucros.

Dessa maneira, hodiernamente, o gerenciamento de dados deve ser encarado por seu aspecto dinâmico, pois, à medida que o Big Data evolui, mais as empresas possuem capacidade de coletar dados inicialmente desconexos e, a partir deles, extrair informações pessoais sobre indivíduos. Assim, dados que hoje não têm a capacidade de identificarem indivíduos podem, no futuro, vir a identificá-los.

Explicando mais a fundo, atualmente o indivíduo pode retirar o seu consentimento para que a empresa pare de tratar os seus dados. Ela, por sua vez, para não eliminar totalmente o dado pode simplesmente anonimizá-lo, isto é, retirar a capacidade de associação do dado em relação ao indivíduo que retirou o seu consentimento. No entanto, isso não impede que no futuro, com o desenvolvimento tecnológico e do Big Data, seja possível haver a reidentificação do dado em relação ao indivíduo.

Assim, o poder do consentimento do usuário fica mais uma vez mitigado, pois atualmente é muito difícil que o titular gerencie totalmente os seus dados, pois o Big Data se apresenta como um mecanismo extremamente poderoso e capaz de relacionar dados inicialmente inúteis e desconectados.

Nesse sentido, o poder decisório do indivíduo passa a ser fictício, pois dá a ele a falsa sensação de controle completo sobre os seus dados, quando na verdade eles ainda estão espalhados na rede mundial de computadores e podem ser utilizados por corporações que consigam fazer um bom uso do Big Data, o que, por fim, prejudica o efetivo direto à privacidade e à proteção de dados pessoais.

Por esse prisma, chegamos à conclusão que, embora o consentimento e a ideia de autodeterminação informativa sejam válidas e importantes, eles por si só não garantem uma proteção adequada ao indivíduo, tendo em vista as limitações mencionadas, quais sejam, a dificuldade de leitura das políticas de privacidade no ambiente online, o uso de estratégias pelo agente de tratamento para conseguir o consentimento do usuário, a assimetria de poderes entre o agente de tratamento e o titular, e o desenvolvimento do Big Data e a dificuldade cada vez maior de gerenciamento de dados pelo titular.

Assim, a seguir vamos analisar estratégias que podem ser implementadas, de modo a suprir as lacunas deixadas pelo foco excessivo no consentimento e garantir, de forma efetiva, a proteção aos direitos fundamentais da privacidade e da proteção de dados pessoais na internet.

7. ESTRATÉGIAS PARA COMPLEMENTAR O CONSENTIMENTO

Como vimos no tópico anterior, embora o consentimento do titular seja imprescindível e relevante para a proteção de dados, ele por si só não é suficiente para garantir a proteção de dados do titular, tendo em vista suas contundentes limitações. Desse modo, é necessário complementá-lo com outras estratégias, que serão destrinchadas a seguir.

7.1. Privacy By Design

O *privacy by design* consiste em uma nova forma de encarar a privacidade e a programação de sites. Por seu termo, ele significa privacidade desde a concepção, ou seja, a ideia da privacidade pensada durante todo o processo de construção do próprio software. Assim, questões atinentes à privacidade e à proteção de dados estariam sendo priorizadas desde a concepção do projeto.

Com base nessa ideia, é preciso incentivar o desenvolvimento do desenho de sistemas tecnológicos seguros, de modo a assegurar a presença de princípios que guiem a proteção de dados não só nas leis, mas também nos próprios sistemas tecnológicos (RUBINSTEIN, 2011, apud MENDES, 2020, p. 521). Embora esteja sendo bastante discutido atualmente, o *privacy by design* não é propriamente um conceito novo. Ele foi inicialmente trabalhado pela canadense Ann Cavoukian, Comissária de Informação e Privacidade de Ontário, na década de 1990.

De acordo com a autora, o *privacy by design* é baseado em sete princípios fundamentais, quais sejam: (1) Proativo, não Reativo, Preventivo e não Corretivo. Ou seja, o projeto precisa se antecipar às violações à privacidade e atuar para que elas não aconteçam, de modo que ocorra constantemente o monitoramento dos riscos; (2) Configuração-padrão, isto é, devem ser criadas medidas de privacidade diretamente em qualquer sistema de tecnologia da informação, com medidas de segurança estabelecendo um privilégio mínimo às empresas, a separação de funções e um controle de acesso obrigatório; (3) Incorporação ao Projeto, o qual aduz que a privacidade deve ser incluída no próprio design e arquitetura dos sistemas, além de aplicar práticas para garantir a segurança do software. Por esse relevante princípio, a privacidade deve estar embutida no projeto desde o começo, e não posteriormente.

A autora ainda complementa citando o princípio da (4) Soma Positiva, que afirma que a implementação da privacidade a determinado sistema deve ser feita de modo que não

prejudique a funcionalidade. Assim, tal funcionalidade deve funcionar como uma soma positiva, e não como uma soma-zero. Portanto, por esse princípio temos que a empresa não pode restringir o acesso a produtos e serviços em troca de uma mitigação da privacidade do usuário; (5) Segurança de Ponta a Ponta, ou seja, deve-se garantir o gerenciamento do ciclo de vida das informações do início ao fim, com confidencialidade, integridade e disponibilidade de informações para todas as partes interessadas.

Além disso, temos a (6) Visibilidade e Transparência, por meio da qual os componentes dos sistemas de TI, assim como as operações dos negócios, devem ser visíveis e transparentes tanto para os usuários quanto para os provedores. E por fim, temos o (7) Respeito pelo Usuário, o qual afirma que, acima de tudo, deve haver respeito e proteção aos interesses do indivíduo.

Com base na análise de todos esses princípios do *privacy by design*, observamos que ele já ajuda a suprir várias limitações do consentimento. Inspirada nessas ideias, as empresas devem, por exemplo, adotar uma linguagem mais amena e suave, não usando o tom de persuasão para tentar convencer o titular a dar o seu consentimento. Assim, coloca-se em prática um respeito maior pelo usuário, que tem o direito de ler as políticas de privacidade de forma mais imparcial, sem haver uma clara tentativa do agente de tratamento de obter o seu consentimento a qualquer custo.

Ademais, com o *privacy by design* as corporações podem elaborar políticas de privacidade com linguagem mais agradável e compatível com o ambiente online, reduzindo tecnismos em prol do entendimento de todos. Para facilitar a absorção do conteúdo e reduzir o excesso de informações, as empresas podem elaborar vídeos explicando seus termos de uso e suas políticas de privacidade.

Atualmente, plataformas como Google e Facebook já possuem esses vídeos, no entanto, eles são bastante curtos e resumidos. Além disso, eles só estão em inglês, o que dificulta o entendimento de grande parte da população. A bem da verdade é que eles possuem legenda em português, mas grande parte dos brasileiros não estão habituados a ver vídeos legendados. De acordo com uma pesquisa feita pelo Instituto Data Popular, em 2020, e publicada no site Vision Business, 76% da Classe C prefere ver filmes dublados na televisão. Além do mais, a mesma pesquisa constatou que 84% dos jovens preferem assistir a conteúdos dublados na Netflix. Sendo assim, a ausência de vídeos em português explicando a política de privacidade de determinado site representa um grande problema a ser enfrentado por essas empresas.

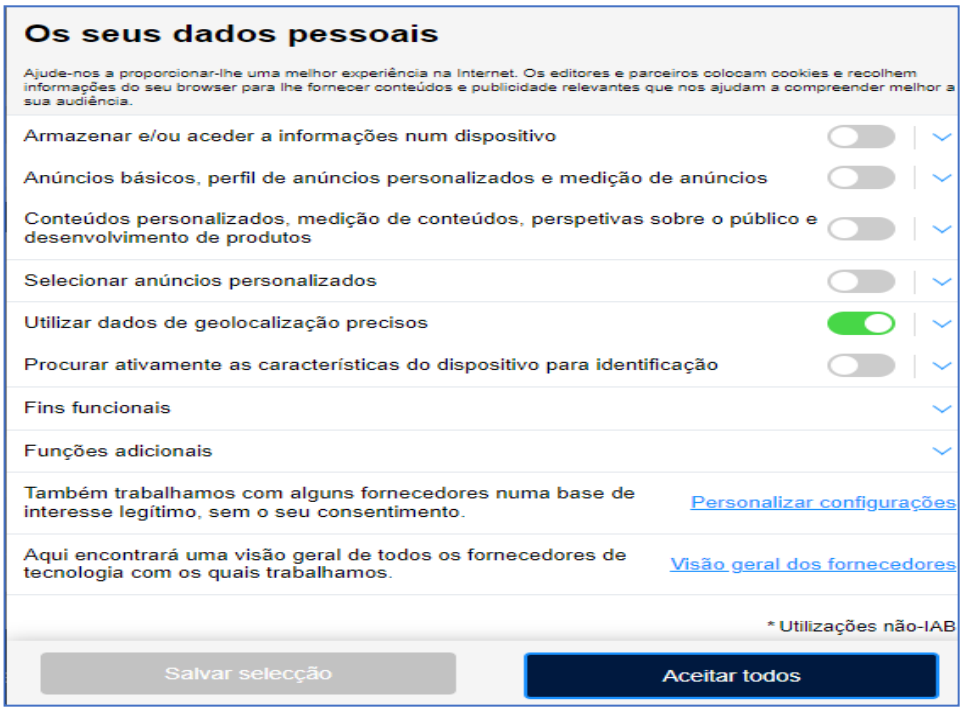
Outra medida a ser adotada pelas instituições para estarem guiadas pelo *privacy by design* seria melhorar o *layout* de seus sites para facilitar o encontro dos termos de uso e das

políticas de privacidade. Já que o intuito é adotar a privacidade desde a concepção e aplicá-la no desenho do sistema, então o acesso a esses conteúdos deveria ser facilitado. Atualmente, na ampla maioria dos sites eles estão na parte mais escondida possível, em letras minúsculas. O ideal seria que eles estivessem em destaque no site, sendo de fácil acesso por todos.

Outrossim, a ideia do *''take it or leave it''* deve ser completamente eliminada. Sendo assim, o usuário não deve ser proibido de acessar o conteúdo, e tampouco deve ter seu acesso limitado no site apenas porque não consentiu para o tratamento dos seus dados. Dentro desse contexto, muitas empresas utilizam o artifício de não proibir diretamente o acesso ao conteúdo, mas sim de torná-lo extremamente incômodo para o usuário, com a caixa pedindo para o titular concordar com o tratamento dos dados ocupando toda a interface do site, o que na prática impede o indivíduo de acessar as informações.

Outro caso de boa política de proteção de dados e inspirada no *privacy by design* a ser adotada por todas as corporações é a elaboração de checklists de privacidade, que funcionam como uma central de monitoramento, por meio do qual o indivíduo consegue acessar com clareza e de forma concentrada a forma como os seus dados são tratados pela respectiva corporação, de modo que pode personalizar o que ele permite que seja trabalhado. O *Google Dashboard* é um exemplo desse caso, mas ele ainda não é tão efetivo, pois, diante da complexidade do Google, é difícil armazenar em um só local todas as informações tratadas dos indivíduos. Mas um dos casos em que isso ocorre com mais precisão é no site *Transfermarkt*, especializado em estimar o valor de mercado dos jogadores de futebol. Conforme observamos na figura abaixo, ele apresenta um checklist bem explicado e intuitivo, no qual o usuário pode consentir livremente.

Figura 1- TRANSFERMARKT



Fonte: Site Transfermarkt, 2022.

Além disso, os agentes de tratamento não podem esquecer de investirem em segurança, de modo a proteger os dados dos usuários de *hackers* e invasores. Sobre isso, destaca-se a política de criptografia de ponta a ponta do WhatsApp, que busca proteger as conversas dos usuários contra terceiros indesejáveis.

Destaca-se, ainda, que com a implementação efetiva dos princípios do *privacy by design*, outra importante limitação do consentimento que será aprimorada é a assimetria presente entre agente de tratamento e usuário. Por óbvio que ainda existirão desigualdades na relação, tendo em vista o poder das grandes empresas e corporações. No entanto, elas serão atenuadas, pois com o *privacy by design* as próprias empresas, desde o princípio, tomarão a privacidade dos usuários como prioridade. Assim, ela pode atuar como uma parceira do titular, ao seu lado para que possa conciliar de forma mais efetiva o direito de trabalho da empresa e os direitos fundamentais dos titulares.

7.2. Análise de risco e responsabilização por meio dos relatórios de impacto: a união entre controlador e Estado

Uma das estratégias para complementar o consentimento e garantir mais respeito aos direitos fundamentais dos usuários é a adoção das ideias de análise de risco (*risk analysis*)

e responsabilização (*accountability*), que consistem justamente na ideia de que a responsabilidade pela proteção de dados pessoais no ambiente digital não pode ficar restrita ao gerenciamento exclusivo do indivíduo por meio de seu consentimento, mas deve ser compartilhada entre todos os atores (MENDES, 2020, p. 522), o que envolve também as empresas e o Estado.

Nesse sentido, o consentimento do titular é importante e não deve ser eliminado. No entanto, para garantir uma máxima proteção aos indivíduos, é necessário que as empresas tenham mecanismos para identificar previamente os riscos, fazer uma análise de todos eles e assumir a responsabilidade por eventuais violações aos dados dos titulares, o que inclui a adoção de medidas para reduzir tais riscos.

A própria Lei Geral de Proteção de Dados tem mecanismos nesse sentido, principalmente mediante os relatórios de impacto, expressos no art. 5º, inciso XVII da LGPD nos seguintes termos:

> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; (BRASIL, 2018).

Dessa forma, com base na análise do dispositivo acima referenciado, cabe ao controlador documentar todos os processos de tratamento de dados que podem causar violações às liberdades civis e direitos fundamentais dos usuários. Essa previsão é extremamente relevante, pois mobiliza as empresas a efetivamente tomarem medidas para protegerem os indivíduos, especialmente nos casos potencialmente mais danosos.

Complementando, o mais interessante de toda essa estratégia é que ocorre a atuação estatal por meio da Autoridade Nacional de Proteção de Dados (ANPD), que poderá analisar os relatórios e requerer ao controlador que elabore esses documentos. Sobre o assunto, a própria LGPD dispõe:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Assim, estamos diante da imprescindível união entre empresa e Estado. A corporação, baseada nas ideias de análise de risco e responsabilização, toma medidas para

averiguar com precisão quais os potenciais riscos envolvidos no tratamento de dados, sempre buscando formas de mitigá-lo e assumindo responsabilidades em relação a violações de dados ocorridas no tratamento. Além disso, atua registrando essas informações e elaborando relatórios de impacto. O Estado, por sua vez, atua analisando os relatórios de impacto e solicitando outros, de modo a averiguar com precisão os riscos envolvidos em determinado tratamento, investigando empresas omissas e displicentes e estabelecendo diretrizes a serem seguidas por todos os envolvidos no tratamento.

Dessa maneira, chegamos à conclusão de que estamos diante de um verdadeiro tripé da proteção de dados no Brasil, formado por titular, controlador e Estado. Com eles três atuando com sinergia, certamente a privacidade e a proteção de dados dos indivíduos serão protegidas. Dito isso, cabe destacar que o titular já está devidamente empoderado pelo poder de seu consentimento e de sua autodeterminação informativa. O controlador, desde o princípio, está em situação de poder por ter a capacidade de elaborar suas políticas de privacidade e terem significativa liberdade para realizarem o tratamento. O Estado, por outro lado, ainda está se desenvolvendo nesse sentido. Logo, para efetivamente termos uma proteção de dados no Brasil, é necessário cada vez mais haver um empoderamento da Autoridade Nacional de Proteção de Dados.

7.3. Fortalecimento da Autoridade Nacional de Proteção de Dados

A Autoridade Nacional de Proteção de Dados foi criada em 2018 para promover o aumento da privacidade e da proteção de dados no Brasil, sobretudo no tocante à fiscalização e efetividade da Lei Geral de Proteção de Dados.

Durante muito tempo ela compreendeu um mero órgão da Administração Pública Federal. Essa condição, por si só, gerou grande desvantagem para a ANPD, tendo em vista que ela não possuía uma completa independência administrativa e funcional, estando em condição de vulnerabilidade e podendo sofrer interferências, notadamente da União. Assim, o fato de a ANPD depender das dotações orçamentárias da União e estar subordinada pela hierarquia impede sua autossuficiência e um trabalho totalmente efetivo em relação à proteção de dados no Brasil.

No entanto, essa realidade está mudando, tendo em vista que a Mesa Diretora do Congresso Nacional promulgou no dia 26 de outubro de 2022 a Lei nº 14.460, que converte a Medida Provisória nº 1.124/22 em lei ordinária. Essa nova lei mantém a competência e a estrutura organizacional, mas converte a ANPD em autarquia de natureza especial, com

autonomia administrativa e financeira. Atualmente a Autoridade Nacional de Proteção de Dados está definida no art. 55-A da Constituição Federal, o qual afirma que ‘’ Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.’’ (BRASIL, 2018).

Assim, a ANPD passa a ter personalidade jurídica, além de seu próprio patrimônio, com funcionamento semelhante às agências reguladoras. Dessa forma, possui muito mais liberdade para trabalhar em prol da proteção de dados dos indivíduos, de forma muito mais autônoma em relação a pressões políticas, por exemplo.

Até porque, em muitos casos a ANPD lida com grandes empresas, que por vezes possuem influência em diversos países do mundo. Essas grandes corporações têm todas as condições de realizarem pressão política para escapar da fiscalização e de punições em caso de violações aos dados de usuários. Nesse caso, uma ampla autonomia orçamentária e jurídica faz-se extremamente necessária para uma atuação plena e eficiente da ANPD, o que a deixa empoderada na missão de dar efetividade para a Lei Geral de Proteção de Dados.

Nesse sentido, o trabalho da ANPD para analisar com tranquilidade os relatórios de impacto dos controladores será muito mais eficiente. A autarquia passará a ter mais liberdade para requerer relatórios de impacto de controladores, de modo a assegurar o cumprimento das medidas necessárias para proteger o tratamento de dados dos usuários. Além do mais, sabendo da existência de um ente forte e autônomo, as empresas certamente terão mais cuidado tanto no tratamento dos dados em si, quanto no momento de realizar a adequada documentação para elaborar o relatório de riscos. O resultado disso tudo é um ganho de segurança para os titulares, que passarão a ter seus dados mais bem cuidados tanto pelos controladores, quanto pela ANPD.

De mais a mais, destaca-se que uma ANPD forte e independente permitirá que ela aprimore até mesmo o consentimento dos usuários, pois assim ela fiscalizará melhor cláusulas obscuras de contratos e conseguirá dar mais contexto ao consentimento. Explicando melhor, ocorre que atualmente o consentimento muitas vezes é coletado de maneira formal, supostamente seguindo os padrões da LGPD. Todavia, várias vezes eles são eivados de vícios mais subjetivos, em que apenas uma análise do contexto possibilita entender se aquele consentimento foi dado de forma totalmente ciente ou não. Com a ANPD tendo mais recursos e atuando de forma mais livre, ela certamente conseguirá ter condições de realizar uma fiscalização mais eficiente dos controladores, de modo a conferir uma eficácia material ao consentimento.

Outrossim, é necessário destacar ainda que, apesar de todos os esforços legislativos

para dar mais autonomia e liberdade para a ANPD, seria interessante que a sociedade civil e o poder político dessem apoio e empoderassem moralmente a Autoridade Nacional de Proteção de Dados. Assim ela se consolidaria ainda mais como centro de poder de tomadas de decisão. Hoje observamos na sociedade brasileira alguns casos de sucesso, como o da Agência Nacional de Vigilância Sanitária (ANVISA), uma autarquia de regime especial que, além da base legislativa, possui o apoio moral do poder político e da sociedade para atuar com eficiência em prol da saúde da população. O mesmo pode acontecer com a ANPD que, uma vez amparada por todos, terá a plena capacidade de atuar em prol de um dos bens mais valiosos dos indivíduos na modernidade: seus dados.

Desse modo, forma-se o tripé da proteção de dados no Brasil. O primeiro ente é o próprio titular, empoderado pela própria LGPD como dotado de autodeterminação informativa devido ao poder do seu consentimento. O segundo seria as empresas, com técnicas de *privacy by design*, *risk analysis* e *accountability* que as tornarão também uma parte ativa da busca pela privacidade e proteção de dados no Brasil, trabalhando desde a concepção e analisando os riscos e assumindo responsabilidades para proteger esses direitos fundamentais. E em terceiro a Autoridade Nacional de Proteção de Dados, que trabalhará com autonomia e independência para fiscalizar os controladores, requerer os relatórios de impacto e cuidar com mais eficiência dos dados de todos os brasileiros.

8. CONSIDERAÇÕES FINAIS

O presente trabalho realizou uma pesquisa legislativa, doutrinária e de artigos, notícias e políticas de privacidade de diversos sites para entender como funciona a proteção de dados no Brasil, notadamente no tocante à proteção de direitos fundamentais.

Inicialmente foi realizada uma análise histórica e conceitual do direito fundamental à privacidade, onde foi constatado um crescimento relevante desse direito com o passar do tempo, especialmente no século XIX, com a publicação do artigo *Right to privacy*, escrito por Samuel Dennis Warren e Loius Dembitz Brandeis. No entanto, com o passar do século XX, mudanças tecnológicas e estruturais da sociedade foram gerando uma coleta cada vez mais intensa dos dados das pessoas. Assim, o direito à privacidade foi evoluindo e gerando ainda um outro direito, o da proteção de dados pessoais, positivado como um direito fundamental com a Emenda Constitucional 115/2022.

Antes disso, porém, diversas leis já procuravam garantir a privacidade e a proteção de dados dos indivíduos, como a Lei Carolina Dieckmann, o Marco Civil da Internet e, principalmente, a Lei Geral de Proteção de Dados, que entrou em vigor em 2020, conferindo uma proteção muito maior para a segurança dos dados no Brasil, com o estabelecimento de princípios, diretrizes e dispositivos para regular o tratamento dos dados no Brasil, além de estabelecer alguns conceitos importantes, como o de dados pessoais, dados sensíveis, titular, controlador, agentes de tratamento e relatórios de impacto.

Observou-se também que a LGPD se pauta pelo princípio da autodeterminação informativa, em que dá ao titular o centro do poder decisório. Na ampla maioria dos casos é ele quem decide se seus dados serão ou não tratados pelo controlador, o que faz com que o consentimento do titular ocupe um lugar de destaque na LGPD e para a proteção de dados no Brasil. Ocorre que esse método pautado com grande ênfase no consentimento, embora tenha gerado grandes avanços, possui algumas limitações, não sendo totalmente efetivo.

Nesse caso, algumas das principais limitações do consentimento a serem destacadas são a dificuldade de leitura das políticas de privacidade no ambiente online, o uso de estratégias pelos agentes de tratamento para obter o consentimento, a assimetria de poderes na relação entre controlador e titular e o desenvolvimento acentuado do Big Data e a dificuldade progressiva de gerenciamento dos dados.

Para a superação dessas estratégias e dar mais efetividade para o próprio consentimento, foram analisadas as técnicas do *privacy by design*, do *risk analysis* e do

accountability, além do uso de relatórios de impacto, de modo que as próprias empresas, desde o princípio, pautariam suas ideias pelo direito à privacidade e proteção de dados dos usuários, programando o desenho de seus sites e usando uma linguagem mais direcionada para o respeito aos indivíduos, utilizando checklists personalizáveis e evitando más condutas, como o impedimento do acesso ao conteúdo por aqueles usuários que não aceitaram as políticas de privacidade ou não disponibilizaram seus dados pessoais para o controlador.

Além do mais, faz-se necessário um empoderamento da Autoridade Nacional de Proteção de Dados, atualmente uma autarquia em regime especial responsável por fiscalizar as empresas e estabelecer diretrizes a serem seguidas por todos. Além disso, ela tem a capacidade de requerer relatórios de impacto dos controladores, de modo que ocorra uma fiscalização maior das empresas, especialmente nos casos potencialmente mais danosos à privacidade dos indivíduos.

Assim, chegamos à conclusão de que a ideia do consentimento como base central da LGPD é apenas parcialmente efetiva, possuindo algumas limitações. Sendo assim, é necessário que as empresas adotem todas as medidas possíveis para evitar violações aos dados dos usuários e que o Estado atue fortemente por meio da ANPD para conferir ainda mais segurança aos indivíduos. Dessa forma, estamos diante do tripé da proteção de dados no Brasil, formado por uma atuação conjunta entre o titular, as empresas e o Estado, que devem atuar de forma integrada e harmônica para garantir, efetivamente, os direitos fundamentais da privacidade e da proteção de dados na internet.

REFERÊNCIAS

AMAZON. **Notificação de Privacidade da Amazon**. Ajuda e Serviço de atendimento ao cliente. São Paulo. 2022. Disponível em https://www.amazon.com.br/gp/help/customer/display.html?nodeId=201283950&ref_=footer_privacy Acesso em 27 de out. 2022.

AUXIER, Brooke et al. **Americans and privacy: Concerned, confused and feeling lack of control over their personal information**. Pew Research Center. 2019. Disponível em https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf Acesso em 23 de out. 2022

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Gen, Editora Forense, 2019.

BRASIL, **LEI Nº 10.406, DE 10 DE JANEIRO DE 2002**. Institui o Código Civil. Brasília, Casa Civil, 2002.

BRASIL, **LEI Nº 8.069, DE 13 DE JULHO DE 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, Casa Civil, 1990.

BRASIL. Autoridade Nacional de Proteção de Dados. **Congresso Nacional promulga a Lei nº 14.460 que transforma a ANPD em autarquia de natureza especial.** Notícia. Brasília. 2022. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/congresso-nacional-promulga-a-lei-no-14-460-que-transforma-a-anpd-em-autarquia-de-natureza-especial Acesso em 01 de nov. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Proteção de Dados Pessoais agora é um direito fundamental.** Notícia. Brasília. 2022. Disponível em https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental Acesso em 14 de set. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL**. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, Casa Civil, 2012.

BRASIL**. LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, Casa Civil, 2014.

BRASIL**. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, Casa Civil, 2002.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência (Florianópolis), p. 213-239, 2017.

CARVALHO, Gisele Primo; PEDRINI, Taina Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. **Revista da ESMESC**, v. 26, n. 32, p. 363-382, 2019.

DE SOUSA, Jéffeson Menezes. **A Efetividade Da Proteção De Dados Pessoais Frente Ao**

Big Data. Dissertação. Universidade Tiradentes. Aracaju. 2017

DE SOUZA, **Ramon. Brasileiros se preocupam com segurança, mas não leem termos de uso, diz pesquisa**. Segurança. CanalTech. São Paulo. 2021. Disponível em https://canaltech.com.br/seguranca/brasileiros-se-preocupam-com-seguranca-mas-nao-leem-termos-de-uso-diz-pesquisa-183554/ Acesso em 23 de out. 2022.

DE TEFFÉ, Chiara Antonia Spadaccini; TEPEDINO, Gustavo. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83, 2020.

DOS SANTOS, Gidevaldo Novais. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. **Revista de Ciência da Computação**, v. 4, n. 1, p. 34-39, 2022.

EGO, Globo**. Vazam fotos íntimas da atriz Jennifer Lawrence.** Notícias. Famosos. São Paulo. 2014. Disponível em http://ego.globo.com/famosos/noticia/2014/08/vazam-fotos-intimas-da-atriz-jennifer-lawrence.html Acesso em 14 de set. 2022.

ELSHOUT, Maartje et al. **Study on consumers' attitudes towards terms and conditions (T&Cs). Final report**. European Commission, 2016.

FACEBOOK. **Política de Privacidade**. Privacy. Policy. São Paulo. 2022. Disponível em https://www.facebook.com/privacy/policy Acesso em 23 de out. 2022.

FAYE. **What does your phone know about you?** Blog. Thinkmoney. Londres. 2020. Disponível em https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/ Acesso em 27 de out. 2022.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2020.

FIORILLO, Celso Antonio Pacheco. **O Marco Civil da Internet e o meio ambiente digital na sociedade da informação: Comentários à Lei n. 12.965/2014**. Saraiva Educação SA, 2017.

G1, Globo**. Apple retoma 1º lugar em ranking de marcas mais valiosas do mundo; Louis Vuitton lidera entre marcas de luxo.** Notícias. Economia. São Paulo. 2022. Disponível em https://g1.globo.com/economia/noticia/2022/07/04/apple-retoma-1o-lugar-em-ranking-de-marcas-mais-valiosas-do-mundo-louis-vuitton-lidera-entre-marcas-de-luxo.ghtml Acesso em 05 de out. 2022.

GABRIEL, Martha. **Marketing na era digital: conceitos, plataformas e estratégias**. Novatec Editora, 2010.

GONÇALVES DA SILVA, Lucas; DA ANUNCIAÇÃO MELO, Bricio Luis. A Lei Geral de Proteção de Dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico. **Revista Jurídica (0103-3506)**, v. 3, n. 56, 2019.

GOOGLE, **Política de Privacidade do Google**. *Policies*. Pivracidades e Termos. 2022. Disponível em https://policies.google.com/privacy?hl=pt-BR&fg=1 Acesso em 17 de out. 2022

IDCÁTEDRA, Instituto Cátedra. **GDPR: o que é e qual a diferença em relação à LGPD?** Blog. São Paulo. 2021. Disponível em https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-

diferenca-em-relacao-a-lgpd/#:~:text=A%20LGPD%20exige%20registro%20de,sujeitas%20%C3%A0%20manuten%C3%A7%C3%A3o%20de%20registros.&text=A%20LGPD%20exige%20que%20o,de%20certas%20atividades%20de%20tratamento. Acesso em 02 de set. 2022.

KHOURI, Paulo R. Roque A. O problema do consentimento informado na Lei Geral de Proteção de Dados Pessoais. **Revista Consultor Jurídico**, 2021. Disponível em https://www.conjur.com.br/2021-mar-31/garantias-consumo-problema-consentimento-informado-lgpd#:~:text=O%20fato%20%C3%A9%20que%2C%20a,conte%C3%BAdo%20dos%20termos%20de%20uso. Acesso em 25 de out. 2022.

MANN, Dillon. **Marco Civil: Statement of Support from Sir Tim Berners-Lee**. World Wide Web Foundation, v. 24, 2014.

MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. **Revista Eletrônica Direito e Política**, v. 15, n. 3, p. 955-984, 2020.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. **Isjlp**, v. 4, p. 543, 2008.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. Saraiva Educação SA, 17. ed. São Paulo. 2022.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor-Linhas gerais de um novo direito fundamental**. Saraiva Educação SA, 2014.

MENDES, Laura Schertel; DA FONSECA, Gabriel C. Soares. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI-Revista Estudos Institucionais**, v. 6, n. 2, p. 507-533, 2020.

MERCADO LIVRE. **Política de Privacidade.** Privacy. Policy. São Paulo. 2022. Disponível em https://www.mercadolivre.com.br/privacidade Acesso em 29 de out. 2022.

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

NEVES, Rebeca de Aguilar Pereira. **GDPR e LGPD: estudo comparativo**. Trabalho de Conclusão de Curso; Centro Universitário de Brasília – UniCEUB. Brasília. 2021.

OCI, Oracle. **O que é Big Data?**. Big Data. São Paulo. 2022. Disponível em https://www.oracle.com/br/big-data/what-is-big-data/ Acesso em 27 de out. 2022.

OEA, Organização dos Estados Americanos, **Convenção Americana de Direitos**. Humanos (Pacto de San José de Costa Rica), 1969.

ONU, Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: https://www.unicef.org Acesso em 10 de out. 2022.

PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018: uma análise dos**

principais aspectos e do conceito privacidade na sociedade informacional. Trabalho de Conclusão de Curso. Universidade Federal do Paraná. Curitiba. 2019.

PEÑA. Paz; VARON, Joana; **O poder de dizer NÃO na Internet: Um olhar feminista para o consentimento em tecnologias digitais**. Coding Rights. 2019. Disponível em https://medium.com/codingrights/o-poder-de-dizer-n%C3%A3o-na-internet-17d6e9889d4a Acesso em 29 de out. 2022.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**. 3ª Edição 2021. Saraiva Educação SA, 2021.

PINTO, Carolina Huff. **Relação do algoritmo com a publicidade nas mídias sociais**.Trabalho de Conclusão de Curso; Centro Universitário de Brasília – UniCEUB. Brasília. 2015.

PIRES, Leonardo Thadeu. A Lei Geral de Proteção de Dados e a validade da cláusula de consentimento. Opinião. **Revista Consultor Jurídico**. 2021. Disponível em https://www.conjur.com.br/2021-set-11/pires-lgpd-validade-clausula-consentimento Acesso em 30 de out. 2022.

PONTICELLI, Murilo Meneghel. **O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da Lei Geral de Proteção de Dados**. Monografia. Universidade do Sul de Santa Catarina. Tubarão, 2018.

PORTUGUAL. **Constituição da República Portuguesa**. Diário da República n.º86/1976. Lisboa. 1976

ROMERO, Luiz. **Não li e concordo.** Super. Editora Abril. São Paulo. 2017. Disponível em https://super.abril.com.br/tecnologia/nao-li-e-concordo/ Acesso em 30 de out. 2022.

SAMUEL, D. Warren & Louis D. Brandeis, The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193, 1890.

SANTOS, Dhiulia de Oliveira. **A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018)**. Trabalho de Conclusão de Curso; Centro Universitário de Brasília – UniCEUB. Brasília. 2019.

SARLET, Ingo Wolfgang; DONEDA, Danilo; MENDES, Laura Schertel. **Estudos sobre Proteção de Dados pessoais**. Saraiva Educação SA, 2022.

SOARES, Rafael Ramos**. Lei geral de proteção de dados–LGPD: direito à privacidade no mundo globalizado.** Trabalho de Conclusão de Curso. Pontifícia Universidade Católica de Goiás. Goiania. 2020.

TATEOKI, Victor Augusto. A proteção de dados pessoais e a publicidade comportamental. **Revista Juris UniToledo**, v. 2, n. 01, 2017.

TEIXEIRA, Tarcísio. **LGPD e Commerce**. 2. ed. São Paulo: Saraiva, 2021.

TRANSFERMARKT. Site. **Política de Privacidade**. 2022. Disponível em https://www.transfermarkt.com.br/ Acesso em 01 de nov. 2022.

UOL. **"Fica uma sensação de faca no peito", diz Carolina Dieckmann sobre fotos roubadas**.

Notícias. Celebridades. São Paulo. 2012. Disponível em http://celebridades.uol.com.br/noticias/redacao/2012/05/14/sensacao-de-faca-no-peito-diz-carolina-dieckmann-sobre-fotos-publicadas.htm Acesso em 29 de ago. 2022.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação – (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, UNB, Brasília, 2007. **Postagem de**, v. 21, 2007.

WHATSAPP. **Sobre a criptografia de ponta a ponta.** Privacidade e segurança São Paulo. 2022. Disponível em https://faq.whatsapp.com/791574747982248/?locale=pt_BR Acesso em 30 de out. 2022.

WILLIAM. **Como os algoritmos são usados na internet e nas redes sociais.** Médium. 2021. Disponível em https://medium.com/resumos-resenhas/como-os-algoritmos-sao-usados-nas-redes-sociais-8d38021ef8fe Acesso em 30 de out. 2022.

SCHIAVO. **ANPD passa a ser autarquia de natureza especial**. Lee, Brock, Camargo Advogados. 2022. Disponível em https://lbca.com.br/anpd-passa-a-ser-autarquia-de-natureza-especial/ Acesso em 02 de nov. 2022.