JOÃO ANTÔNIO DIAS DA COSTA FEIJÓ

A VALIDADE DO CONSENTIMENTO DOS USUÁRIOS AOS TERMOS DE USO E POLÍTICAS DE PRIVACIDADE DE APLICAÇÕES DE INTERNET, SOB A ÓTICA DA LEI 13.709/2018.

Santa Maria

2020

.

A VALIDADE DO CONSENTIMENTO DOS USUÁRIOS AOS TERMOS DE USO E POLÍTICAS DE PRIVACIDADE DE APLICAÇÕES DE INTERNET, SOB A ÓTICA DA LEI 13.709/2018.

João Antônio Dias da Costa Feijó[1]
Anarita Araújo da Silveira[2]

RESUMO

O presente trabalho analisa a validade jurídica do consentimento no tocante aos dados pessoais dos usuários de aplicações de internet, a partir do advento, no Brasil, da Lei nº 13.709/2018. Tendo em vista que a Lei Geral de Proteção de Dados segue a diretriz normativa da autodeterminação informacional, portanto, pauta o consentimento do usuário como protagonista das relações jurídicas envolvendo dados pessoais, assim, pergunta-se: este consentimento, uma vez cedido, pode ser considerado efetivamente livre? O presente estudo tem como objetivo geral a análise do consentimento previsto na Lei Geral de Proteção da Dados sob a luz da teoria dos vícios do consentimento. Como objetivos específicos, busca realizar um estudo histórico sobre a evolução do consentimento no Direito da Privacidade de Dados por meio de suas leis ao longo do tempo; Analisar os limites e os usos do consentimento sob a ótica da Lei nº 13.709/2018; Identificar potenciais limitações que a lei brasileira apresenta quanto ao instituto do consentimento, questionando-se sobre se o mesmo pode ser considerado efetivamente livre. O método de abordagem utilizado é o dedutivo. Os métodos de procedimento utilizados são Históricos e Comparativos. Concluiu-se com o estudo, que o consentimento humano no tocante à autodeterminação de dados não é incólume à vícios, levando em consideração aspectos neurológicos, econômicos, e de informação, e que portanto não deveria ser um instrumento norteador no que tange à proteção de dados pessoais, vez que o usuário não está devidamente preparado para dispor livremente de suas informações pessoais na rede de computadores.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados Pessoais. Privacidade. *Surveillence.* Consentimento. Autodeterminação Informacional.

ABSTRACT:

The present work analyzes the legal validity of the consent regarding the personal data of the users of internet applications, from the advent, in Brazil, of the Law nº 13.709/2018.Considering that the General Law of Data Protection follows the normative guideline of the informational self-determination, therefore, guides the user's consent as a protagonist of the legal relations involving personal data. Thus, the question is: can this consent, once given, be considered effectively free? The general objective of the present study is to analyze the consent provided for in the General Data Protection Law in light of the theory of the vices of consent. As specific objectives, it seeks to carry out a historical study on the evolution of consent in the Data Privacy Law through its laws over time; To analyze the limits and uses of consent under the perspective of Law no. 13.709/2018; To identify potential limitations that the Brazilian law presents regarding the institute of consent, questioning whether it can be considered effectively free. The method of approach used is the deductive. The procedure methods used are Historical and Comparative. The study concluded that human consent concerning the self-determination of data is not immune to vices, taking into account neurological, economic, and information aspects, and therefore should not be a guiding instrument with respect to the protection of personal data, since the user is not properly prepared to freely dispose of his personal information on the computer network.

KEYWORDS: General Law of Data Protection. Privacy. Surveillence. Consent. Informational self-determination.

INTRODUÇÃO

O presente trabalho analisará a validade jurídica do consentimento no tocante aos dados pessoais dos usuários de aplicações de internet a partir da análise dos limites e usos constantes dos termos de uso e políticas de privacidade, a partir do advento, no Brasil, da Lei nº 13.709/2018, mais conhecida como LGPD, Lei Geral de Proteção de Dados.

Tal diploma legal, sancionado em agosto de 2018, trouxe cominações acerca de um cenário que emergiu de forma muito rápida nos últimos anos, vez que os dados pessoais, tratados e controlados nas relações cibernéticas, rapidamente constituíram, por meio de ferramentas como *Big Data*, Mineração de Dados, e publicidade direcionada, um modelo de negócio mundialmente difundido na internet, transformando os dados pessoais em um *commodity* muito valioso e uma peça chave para o desenvolvimento de empresas que possuem atuação na internet, entes governamentais e não-governamentais, entre outros atores.

O tema proposto teve sua escolha baseada, de forma primordial, na atual relevância que possui a privacidade como um todo, bem como sua eventual negligência por grande parte da sociedade. Isto porque o ser humano está inserido hoje em um ambiente de extrema exposição *online*. Desta feita, imperiosa se faz a atenção plena do Direito e de e seu dever de regulação e fiscalização, para que se mantenham intactos e bem protegidos os direitos fundamentais que foram arduamente conquistados ao longo da história. bem como, apropriada aplicação pelos entes responsáveis, em que pese o valor pessoal e seus usos.

Subsidiariamente, o crescente interesse pelo tema se justifica pelo clamor social gerado por eventos que envolvem violação de dados pessoais, sejam estes em sede governamental ou em grandes corporações, episódios que sempre demandarão reposta imediata dos ordenamentos jurídicos das nações envolvidas.

Assim, para que seja possível verificar respostas para os desafios apresentados pelo desenvolvimento tecnológico *versus* proteção de dados, devem ser analisadas, de forma exauriente, as leis que lecionam sobre o tema e suas fragilidades e incompatibilidade frente as mais recentes doutrinas e estudos, pois, somente assim, haverá o sucesso da tutela do direito à privacidade.

O Direito da Proteção de Dados Pessoais teve como seu primeiro diploma legal o *Data Act*, instaurado na Suécia nos idos de 1970, e desde então, enquanto comunidade global, promulgaram-se diversos dispositivos legais dedicados ao tema, em especial, na história

recente, a GDPR (*General Data Protection Regulation*) – que é o diploma mais influente da atualidade sobre o tema.

Esta, em vigor na União Europeia desde 2016, faz linha de frente a um movimento global de cuidado ao tema em uma época em que, não raro, grandes corporações valeram-se da fragilidade legislativa e informacional para exercer a livre manipulação de dados pessoais e da própria democracia. Cite-se por exemplo os vazamentos promovidos pelo norte-americano Edward Snowden, em 2013, que deflagaram o poderio vigilante do governo dos Estados Unidos no que tange as relações cibernéticas, tal incidente criou um paradigma para a violação do direito à privacidade de dados pessoais.

Nesta senda, o pleito presidencial norte-americano de 2016 também gerou grave preocupação quanto ao valor que os dados possuem na sociedade atual por meio do escândalo envolvendo a empresa de tecnologia Cambridge Analytica, que - alegadamente, violou cerca de 87 milhões de contas no *Facebook* em prol de seus clientes em campanha, o que denota, não só gravíssima violação de direitos da privacidade, como também a mitigação da própria democracia, já que os movimentos eleitoreiros foram traçados a partir do que se denomina como mineração e mercantilização dos dados pessoais.

Nesse panorama, o poder legislativo brasileiro elaborou a Lei Geral de Proteção de Dados, aprovada no ano de 2018, que, em última análise, faz parte da última geração de leis de dados pessoais por estar em consonância doutrinária com diplomas elaborados na Europa e nos Estados Unidos.

Não obstante, verifica-se que apesar de manifesta importância temática, tais diplomas legais ainda estão presos no mesmo referencial teórico das primeiras gerações de leis – que prega a autodeterminação informacional – que em outras palavras é a centralização da responsabilidade sobre o ato de ceder dados pessoais – no próprio indivíduo, especialmente, no seu consentimento, definindo uma série de elementos que o adjetivam (livre, expresso, inequívoco e com finalidade expressa), para que este seja válido nas relações jurídicas envolvendo dados pessoais.

Critérios como este evocam uma importante reflexão: na atualidade enfrenta-se problemas seguramente inéditos em termos de tecnologia, com instrumentos defasados. Isto se dá pois nas primeiras gerações de leis de dados pessoais, não se vivia uma sociedade em rede, com contratos de termos de uso sendo celebrados por milhões de usuários por segundo, sobretudo, onde a maioria destes serviços são alegadamente, gratuitos, mas são adimplidos pelo usuário por meio de anúncios, moldados a partir de um perfil individualizado. E pior, tais contratos são celebrados pela maioria dos usuários sem sequer serem lidos, tampouco sua

importância é devidamente divulgada pelos veículos de informação. Neste ponto, cabível considerar que o sistema jurídico global possa estar de mãos atadas frente a tecnologias algorítmicas, inteligências artificiais e sobretudo, a própria sociedade informacional.

Ora, se a sociedade está cada vez mais inserida em um conjunto informacional onde a maioria, se não a integralidade das relações, se dão neste meio, a Lei Geral de Proteção de Dados cumpre o seu escopo, ou apenas perfaz uma falsa proteção ao usuário?

Nesse contexto, considerando que vive em uma sociedade informacional, e que são lançadas, todos os dias, informações sensíveis à rede de computadores, como contraprestação ao uso de aplicações e serviços (indiscutíveis facilitadores da vida moderna), o usuário deve ter certeza de que seus dados e seu direito constitucional à privacidade estarão resguardados.

O presente trabalho encontra-se adequado à linha de pesquisa ao colaborar com os novos estudos voltados à esfera dos direitos humanos e fundamentais em face das novas tecnologias, em especial, a privacidade, resguardada pela Constituição Federal e por diversas leis infraconstitucionais, como o Código Civil, O Marco Civil da Internet, o Código de defesa do Consumidor e, por derradeiro, o objeto principal que este artigo analisará, a Lei Geral De Proteção de Dados Pessoais. O método de abordagem a ser utilizado será o dedutivo, vez que utilizará disposições legais e informações coletadas em contexto geral para aplicação em cenário particular. Os métodos de procedimento utilizados serão Históricos e Comparativos.

Capítulo I – Sociedade informacional e a preocupação com a privacidade de dados.

É sabido que se vive em uma sociedade muito diferente daquelas que civilizações antigas outrora viveram nos séculos anteriores, isto muito se deve em grande parte ao desenvolvimento e democratização exponenciais das tecnologias informacionais.

Não demorou muito para que a grande rede de computadores tenha estendido seus tentáculos o suficiente para que todos os utensílios eletrônicos fossem transformados em *smart*, com inúmeras capacidades, entre elas, em especial a de coletar dados pessoais e conectar-se à rede – formar o que conhecemos hoje por Internet das Coisas, conforme pontua (MAGRANI, 2019, p. 296):

> "Na verdade, as coisas da Internet das Coisas não são coisas: são sensores — por mais sexy que a expressão, pela razão e pela forma como foi cunhada, possa aparentar. E porque elas são sensores cada vez mais comuns, pervasivos, próximos e incorporados ao cotidiano do indivíduo, representam risco potencial muito maior para a proteção de seus dados pessoais, da sua privacidade, do seu direito de autodeterminação informativa."

São estes sensores pensantes e de inegável utilidade e praticidade na vida moderna, que

revolucionaram a forma como percebemos a informação, ou que a sociedade informacional nos vigia. Cabível a comparação deste atual ecossistema com a *teletela* Orwelliana, sistema de vigilância governamental possuído por cada indivíduo - retratada no romance "1984". Entretanto, salvo suas semelhanças com a realidade, a noção do Grande-Irmão, que no romance de George Orwell trata-se de um ente governamental e centralizado, não guarda real semelhança com a realidade, já que nos dias atuais a busca pelos dados pessoais gravita em torno de entes privados, em sua gigantesca maioria, o que retrata a ideia de Pequenos Irmãos, ou *Tiny Brothers* (BIONI, 2020).

Em que pese a comparação com uma obra de ficção, a sociedade atual possui traços preocupantes de sinais que podem acarretar problemas no futuro, já que, apesar de não possuir *teletelas* de vigilância governamental, o ser humano contemporâneo, carrega consigo um *smartphone* e por meio dele, firma negócios jurídicos, provavelmente algumas vezes por semana, sempre que utiliza um novo serviço, faz *download* de um novo aplicativo, e sobretudo, alimenta – por intermédio deste dispositivo, imensuráveis bancos de dados pessoais – com os seus próprios dados.

Em um breve conceito, pode-se definir a privacidade de dados como a reivindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros (WESTIN, 1970, p. 7). No mesmo sentido, tais informações deflagram aos olhos das grandes corporações e instituições estatais, os gostos, renda, entre outros padrões que, por derradeiro, definem um perfil individualizado de cada um (SOLOVE, 2007).

Nesse sentido, a preocupação com a privacidade de dados se deu com grande força a partir da década de 1960, especialmente após a ascensão do computador, e gerou um movimento de preocupação com a privacidade - que esteve em voga entre os mais variados campos da ciência, e persiste, pode-se dizer, até os dias atuais. Em última análise, o computador foi desenvolvido para processar dados. Assim, os dados pessoais passaram a ser objeto de análise, quando estes foram percebidos como ferramenta importante primeiramente na esfera governamental, para fins de coordenação e planejamento de ações (BIONI, 2020).

A implementação desta quebra do anonimato causou o que se determina como o estado de sujeição do indivíduo à perda deliberada de seus próprios direitos de privacidade por vontade própria, ou o consentimento em perder sua privacidade como contraprestação às maravilhas oferecidas em troca (BAUMAN, 2014, p. 20).

Assim afirma Manuel Estrada, quanto à preocupação com a privacidade no cenário de Internet das Coisas, abaixo referida como *IoT (Internet of Things)* e Big Data:

> A IoT captura dados a cada minuto em que andamos na rua, estacionamos os nossos carros ou cada vez que usamos um smartphone ou cartão de crédito. À medida que é recolhida cada vez mais informações pessoais, surgem preocupações relativamente aos perfis, discriminação, exclusão, vigilância do governo e perda de controle. Os avanços tecnológicos já ultrapassaram claramente os quadros legais existentes, criando uma tensão entre inovação e privacidade, sempre que as leis não refletem os novos contextos sociais e não garantem os direitos dos cidadãos (ESTRADA, 2016, p.43).

Deste panorama de preocupação é que emergiram leis, cada vez mais específicas, com o condão de tutelar o direito a privacidade dos indivíduos frente a novas tecnologias.

Capítulo II – As gerações de Leis de Proteção de Dados Pessoais e o Consentimento.

Destarte, a seguinte a tabela ilustra o trajeto do consentimento a partir das gerações de leis de proteção aos dados pessoais - e a sua crescente importância nas legislações ao longo do tempo. O movimento que tratou de colocar o usuário, e portanto, seu ato volitivo de dar consentimento, em um local de primeira importância nas relações jurídicas, é o que a doutrina chama de autodeterminação de dados, pela sua natureza centrada na vontade do usuário. Bobbio define a autodeterminação como:

> por liberdade positiva, entende-se — na linguagem política — a situação na qual um sujeito tem a possibilidade de orientar seu próprio querer no sentido de uma finalidade, de tomar decisões, sem ser determinado pelo querer de outros. Essa forma de liberdade é também chamada de autodeterminação (BOBBIO, 1997, p. 51).

Nesse passo, mostra abaixo, a tabela:

Geração	Objetivo e inovação	Paradigma
1ª Geração	Foco no processamento de dados na seara governamental, partiu de uma preocupação em domesticar a tecnologia em decorrência dos avanços e da percepção de que as informações pessoais dos cidadãos constituíam um útil instrumento para o crescimento ordenado (MAYER-SCHONEBERGER, 1997).	Exemplo destas leis de primeira geração são a Lei do Land alemão de Hesse, de 1970; a primeira lei nacional de proteção de dados sueca, que foi o Estatuto para bancos de dados de 1973 – Data Legen 289, ou Datalag, além do Privacy Act norte-americano de 1974 (DONEDA, 2010. P. 41).

2ª Geração	Figura do Grande Irmão é diluída em detrimento da preocupação com o setor privado, sendo a inovação, a tutela dos direitos de privacidade de dados na esfera pública e privada. A segunda geração, portanto, ocorre com a extensão da preocupação aos dados e a incapacidade governamental de gerência de todos os dados pessoais, de forma que a responsabilidade pela proteção de dados passa a ser de responsabilidade de seus titulares (BIONI, 2020, p. 111).	Pode-se dizer que o seu primeiro grande exemplo foi a lei francesa de proteção de dados pessoais de 1978, intitulada Informatique et Libertées (DONEDA, 2010. P 41).
3ª Geração	Não tardou para que se observasse novamente uma mudança de paradigma na matéria: percebeu- se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. A terceira geração de leis procurou sofisticar a tutela dos dados pessoais. (DONEDA, 2010. P. 42). O papel de protagonismo do indivíduo segue a mesma senda, entretanto, incorporou-se a criação de deveres para quem coleta e processa dados pessoais, assim – para um cenário dualista, (BIONI, 2020, p. 111).	Paradigma criado pela Decisão da Corte Constitucional Alemã (BIONI, 2020. P. 111), em 25 de março de 1983, no histórico julgamento da Lei do Censo (Volkszählungsgesetz). Essa lei visava a fornecer informações à Administração Pública no que tange ao crescimento populacional, distribuição espacial da população pelo território e atividades econômicas realizadas no país, sendo feita a coleta de dados dos cidadãos por meio de uma série de questionamentos versando sobre profissão, moradia e local de trabalho (MENDES, 2014, p. 30).

4ª Geração	Esta geração veio para instaurar a criação de autoridades reguladoras independentes para a aplicação das leis de proteção de dados pessoais, bem como de proposições normativas, que não deixavam ao reino do indivíduo a escolha sobre o processamento de certos tipos de dados pessoais (DONEDA, Danilo, 2010).	Diretiva Européia (2002/58) sobre o tratamento e a proteção da privacidade nas comunicações eletrônicas (BIONI, 2020, p. 119).

A tabela supra demonstra, sobretudo, a importância do consentimento do indivíduo nas legislações sobre dados pessoais e a autodeterminação de dados como elemento protagonista. De tal maneira, o legislador europeu, na elaboração da Diretiva Europeia, no limiar da 4ª geração de leis, em seu Artigo 17, tratou de qualificar o consentimento como: cedido por qualquer método apropriado, propiciando um específico, livremente cedido, e informado indicador dos desejos do usuário, incluindo uma caixa de seleção quando visitar um site da Internet. Desta forma, o consentimento deve ser cedido por meio inteligível.

A terceira geração de lei, flexibilizou, pelo menos um pouco, a ideia de autodeterminação informacional – já que permitiu que fossem criados direitos e obrigações recíprocas. A partir disso, as leis de dados possuem como foco dois sujeitos – os titulares dos dados pessoais, e quem processa estes dados.

Inobstante aos avanços normativos e às adoções das boas práticas em termos de privacidade de dados nos vindouros diplomas legais, a evolução da tecnologia seguiu seu exponencial trajeto de popularização, tornando a coleta e os usos de dados pessoais cada vez frequentes, complexos e menos transparentes (BIONI, 2020, p.116).

Nesse passo, quando analisada tal postura legislativa em ceder ao usuário a responsabilidade de dispor sobre seus dados, surge o questionamento sobre a capacidade deste de negociar com os produtos e serviços dos dias atuais, que exaustivamente exigem os dados pessoais como requisito de adesão.

Dessa forma, o movimento legislativo no sentido de adjetivar o consentimento como livre, informado, inequívoco, explícito e/ou específico foi uma fórmula de instrumentalizá-lo ao passo em que as relações jurídicas envolvendo dados pessoais, sobretudo pós-internet, foram se tornando cada vez mais complexas e muito mais volumosas, entretanto, o consentimento do usuário seguiu tendo em si, o mesmo poder de determinar o controle dos dados pessoais.

Leva-se a crer, que hoje em dia, portanto, o usuário que negar seu consentimento, se afastará da sociedade, já que inegavelmente está cada vez mais difícil estabelecer uma distância entre sociedade em rede e fora da rede. Insta pontuar o pensamento de Viktor Mayer-Schonberger– acerca do preço que se paga pela não disponibilização de dados por parte do usuário, que deverá ser pago apenas por aqueles dispostos a viver como ermitões (MAYER-SCHONBERGER, 2013).

Desta forma, há de se analisar mais a fundo este consentimento que possui tão grande importância para este objeto de estudo, a fim de se investigar se este instituto está incólume a vícios, e se o usuário pode se considerar protegido, munido apenas de seu livre arbítrio.

Capítulo III – O Consentimento na nova Lei de Proteção de Dados Pessoais.

No Brasil, o direito à privacidade é tutelado como direito fundamental e está presente na Constituição Federal, que, no tocante ao tema – amplia o rol de direitos relacionados à privacidade, garantindo a preservação da vida privada e da intimidade da pessoa, bem como, quanto à inviolabilidade de domicílio e das comunicações, à saber do Art. 5º, inciso 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", e inciso 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).

Inobstante, fosse eficaz a tutela do direito garantido pela constituição, não haveria cabimento para o debate, tampouco necessidade de elaboração de leis específicas com o fim de proteger os dados pessoais.

Neste passo, a regulação da internet e seus desdobramentos na vida civil, teve início no Brasil com o Marco Civil da Internet, lei 12.965 de 2014 – diploma que possui como um de seus escopos a proteção da privacidade dos usuários e de seus dados pessoais, e posteriormente com a nova Lei Geral de Proteção de Dados Pessoais, Lei 13.709 de 2018, dispositivo que, conforme a tabela demonstrada no capítulo anterior, se encontra na 4ª geração de leis, já que prevê em seu texto a criação de dois órgãos independentes de controle e fiscalização (DONEDA, 2010), quais sejam a Autoridade Nacional de Proteção de Dados – ANPD e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (BRASIL, 2018).

Com efeito, a LGPD trouxe cominações importantes, tendo em vista ser a primeira vez que o país legisla exclusivamente sobre o tema, sobretudo quando o legislador faz referência ao modelo proposto pelas diretiva europeia de 1995 no que tange ao consentimento – quando

se transfere boa parte da responsabilidade sobre a cessão de dados para os próprios usuários detentores dos mesmos, o que chama-se autodeterminação informacional.

Em que pese a definição de consentimento segundo a LGPD, a saber: "Art. 5º Para os fins desta Lei, considera-se: [...] 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)". Em consonância ao referido artigo, na visão de Tepedino, Frazão e Oliva (2019, p. 299) o consentimento representa o seguinte:

> "O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações."

Nesse passo, não obstante a LGPD estar perfilada na quarta geração de leis – seu conceito de consentimento, como sendo livre, informado e inequívoco, traz à baila o questionamento sobre sua efetiva proteção aos usuários da internet, e em última análise, sobre sua própria validade, vez que a maioria dos contratos celebrados nesta esfera para o uso de sites e aplicações se dá por termos de privacidade, ou termos de uso, muitas vezes representados por meras caixas de seleção ou botões de chamada para ação.

Nesta senda, um recente estudo realizado por Tsohou e Kosta (2017, p.19) – que teve por objeto usuários finais de aplicativos *mobile*, conseguiu constatar a ineficácia dos termos de privacidade em perfazer um consentimento válido, informado ou específico, *e.g*:

> "As conclusões do segundo modelo de processo implicam que os indivíduos geralmente não têm consciência da sua privacidade, de como esta pode ser violada, do potencial impacto de tal violação e dos seus direitos de privacidade. Quando perguntados se sabiam que legalmente, que os aplicativos móveis não deveriam rastrear a sua localização a menos que fosse necessário para a sua função, todos os participantes responderam negativamente. Além disso, mesmo após a leitura detalhada das políticas de privacidade, os participantes observaram que ainda não se sentem confiantes de que compreendem o que isto significa em termos de riscos de privacidade e potenciais implicações para eles. Portanto, existe uma lacuna entre o fornecimento de informações sobre os fatos (por exemplo, que tipos de dados são recolhidos) e a transformação destes factos em consciência da privacidade" (TSOHOU; KOSTA, 2017, p. 19).

Nesse sentido, é possível que tal consentimento – o qual deveria ser livremente cedido e inequívoco – não esteja incólume à teoria dos vícios de consentimento, já que o usuário médio da rede de computadores, não ciente de que determinada aplicação constitui, antes de tudo, um

modelo de negócio – pode estar recaindo em erro, ao submeter um formulário repleto de informações sensíveis, do qual os termos de uso não tenham sido sequer lidos, em um ato motivado pela euforia da adesão de um novo serviço. Tal comportamento pode ser impulsionado pelas práticas de *neuromarketing* desenvolvidas por empresas possuem controle sobre as aplicações da grande rede, segundo estudo por Parchen, Freitas e de Meireles:

> Se o *neuromarketing* como técnica voltada ao incremento do consumo irracional, pois incide justamente nos elementos automáticos e inconscientes do cérebro humano, faz com que diminua a capacidade de raciocínio e exacerbe os sentimentos e as emoções em torno de uma tomada de decisão impulsiva, há que se concluir que o necessário ânimo ou vontade ponderada, deliberada e manifestamente exarada pelo consumidor está claramente prejudicada, mitigada ou muitas vezes até mesmo aniquilada por conta da imputação forçada de um mecanismo viciante no cérebro que sequer é perceptível (PARCHEN; FREITAS; de MEIRELES, 2018, p. 22).

Outrossim, tais práticas comerciais levam o usuário a crer que a maioria das aplicações utilizadas na *web* são gratuitas, entretanto, ainda que determinado serviço pareça gratuito, ele não é, já que o usuário o paga por meio de seus dados pessoais. Nesse sentido, difícil se faz a obtenção um consentimento válido, uma vez que não existe interação direta com indivíduos por parte das organizações, além disso, tais entes firmam suas políticas de privacidade em parâmetros não palatáveis aos usuários finais.

Ainda, nesse contexto, também é difícil por em perspectiva o empoderamento do usuário no que tange ao controle de seus dados, e por conseguinte, a uma tomada de decisão válida (BELLAMY; HEYDER, 2015).

Capítulo IV – A eficácia do consentimento sob a ótica da Lei Geral de Proteção de Dados

O Código Civil brasileiro prevê a tutela do que denomina vício de vontade, ou a teoria dos vícios de consentimento, institutos jurídicos que devem ser invocados em contratos dos quais, entre outras hipóteses, alguma das partes incorrer em erro substancial.

Sobre esta hipótese, o Artigo 138 do Código Civil dispõe: são anuláveis os negócios jurídicos quando as declarações de vontade emanarem de erro substancial que poderia ser percebido por pessoa de diligência normal, em face das circunstâncias do negócio (BRASIL, 2002).

Desta forma, o presente estudo considera a hipótese de que os termos de uso dos sites, aplicações, e demais serviços oferecidos na internet, possam fomentar a prática deste tipo de

erro nos usuários – já que a realidade mostra que os dados pessoais constituem ativo estratégico de uma série de modelos de negócios (BIONI, 2020, p. 103) – fato que não é notório e difundido entre os usuários médios.

Neste sentido, o Código de Defesa do Consumidor também dispõe sobre a autonomia e proteção da vontade do indivíduo, no seu art. 46:

> "Os contratos que regulam as relações de consumo não obrigarão os consumidores se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance" (BRASIL, 1990).

Frente à tal proteção, resta claro que os contratos celebrados na internet devem levar em consideração a capacidade de manifestação da vontade do indivíduo, já que, práticas utilizadas na *web* como o *neuromarketing*, técnica que explora caraterísticas cerebrais a fim de potencializar o automatismo e a inconsciência, visam apenas ao consumo desmedido.

Tais práticas acabam por afetar a capacidade de livre arbítrio do indivíduo, já que fazem com que a capacidade de raciocínio seja diminuída em detrimento da tomada de decisão impulsiva, gerada por gatilhos implementados nas aplicações (PARCHEN; FREITAS; de MEIRELES, 2018, p. 22).

Nesta senda, considera-se a hipótese de que o consentimento do usuário é passível de manipulação, e portanto, seu direito constitucional à privacidade e intimidade estejam à disposição do mercado de mineração de dados pessoais para manipulação e indução a um comportamento impulsivo.

Frente aos estudos realizados em usuários *mobile por* Tsohou e Kosta (2017) foi possível constatar que o consentimento cedido em um ambiente virtual não traz clareza sobre a especificidade do tratamento ao qual estará sujeita a informação, tampouco quanto a finalidade, conforme requer o consentimento previsto pela LGPD, a saber, a pesquisa:

> Além disso, outra via possível para a investigação futura que deriva dos resultados seria um esquema de conceptualização do consentimento informado da aplicação móvel que permitisse a medição e a escalada. De acordo com a legislação, para que o consentimento seja válido, tem de ser dado livremente, específico e informado. É necessária mais investigação a fim de produzir documentos legais de forma inteligível que contribuam para o fornecimento do consentimento válido dos utilizadores de aplicações móveis**.** *A exigência legal do consentimento separado dos utilizadores para o processamento de dados de localização não deve ser transformada num trivial "clique clique clique"*, como um dos entrevistados o descreveu muito vividamente. Em vez disso, para além de fornecer informações completas, as aplicações devem oferecer aos utilizadores uma oportunidade real de recusar o seu consentimento para o processamento dos seus dados de localização, em particular quando o processamento de tais dados não for essencial para a prestação do serviço. Por

> conseguinte, a teoria do processo desenvolvido oferece uma visão de como os indivíduos processam a informação dada durante o procedimento de instalação da aplicação móvel (TSOHOU; KOSTA, 2017, p. 19).

Além disso, é necessário que se entenda o quão complexo é - e de que forma se dá o fluxo de informações pessoais na rede. Por exemplo, quanto ao formato conhecido de publicidade direcionada nas redes sociais: existem diversos atores envolvidos que tratam os dados e ajudam a formar um perfil cada vez mais individualizado e próximo do perfil de consumo do cliente.

De modo que, em última análise, a determinação do fluxo informacional é muito difícil mas que torna sua compreensão, ainda que rasa, de extrema importância para o consumidor final, que não deve tratar a rede social, por exemplo, como um serviço gratuito que apenas oferece facilidades sem cobrar uma contraprestação.

Como consequência, o titular dos dados pessoais deveria ter consciência a respeito de todos esses atores e das suas respectivas práticas de mineração de dados para que, ao final, pudesse gerencias as suas informações pessoais (BIONI, 2020, p. 140) – e então exercer a autodeterminação de dados com confiança.

Entretanto, seria ilusório assumir que todos os usuários da *web* contraiam as informações necessárias sobre todos os atores que estão envolvidos na manipulação de dados pessoais, e ainda assim, o sabendo, o ser humano possui barreiras cognitivas que impossibilitariam o seu controle real sobre seus dados pessoais. Desta forma, complementa o estudo de Alessandro Acquisti e Jens Grossklags:

> Mesmo que as pessoas tenham acesso a informações completas sobre seu riscos à privacidade e modos de proteção, eles podem não ser capazes de processar grandes quantidades de dados para formular uma decisão racional e sensível à privacidade. A racionalidade do ser humano é limitada, o que limita nossa capacidade de adquirir e depois aplicar informações. Primeiro, mesmo indivíduos que afirmam estar muito preocupados com seu a privacidade não necessariamente toma medidas para se informar sobre privacidade riscos quando a informação está disponível. Por exemplo, observamos discrepâncias ao comparar se os sujeitos foram informados sobre a política relativa às atividades de monitoramento dos funcionários e estudantes em sua organização com seu nível relatado de preocupação com a privacidade. Apenas 46 por cento das pessoas com alta preocupação com a privacidade afirmaram ter se informaram sobre a existência e o conteúdo de uma política de monitoramento organizacional. Da mesma forma, do grupo de com altas preocupações de privacidade, 41% admitem que raramente lê políticas de privacidade (ACQUISTI; GROSSKLAGS, 2005).

Nesse sentido, é possível que o indivíduo imbuído na capacidade de promover

a autodeterminação de seus dados pessoais, não é capaz de agir com precisão em 100% dos casos, desta forma, a produção legislativa se torna frágil quando submete a este indivíduo o poder do consentimento como ferramenta de sua própria segurança. Assim, a crença de que o ser humano é plenamente capaz de consentir ao controle e tratamento de seus dados pessoais, em um processo genuíno, é posta em dúvida quando levantadas estas hipóteses (BIONI, 2020, p. 141).

Nesse passo, uma vez ventilada a hipótese de que a eficácia do pilar que sustenta diversas normas jurídicas sobre o tema, que é o consentimento - por conseguinte a autodeterminação de dados pessoais, possa não ser capaz de representar a vontade do individuo, e por óbvio, em tal circunstância, não tutelar o seu direito constitucional de privacidade, é imperioso que sejam pensados novos mecanismos jurídicos materiais, se os primeiros paradigmas geracionais da proteção de dados pessoais foram gerados em torno desta alcunha que delega para o usuário da rede de computadores, à mercê de entre outras técnicas, algorítmos de *e-commerce*, a responsabilidade sobre direitos constitucionais.

Capítulo V - Considerações Finais

Em conclusão, o presente trabalho teve por condão explorar possíveis lacunas no sistema legislativo de proteção de dados pessoais, sem contudo, embuído de ambição para apontar soluções definitivas para tais problemas, mas sim buscou trazer a baila discussões que possam, no mínimo, fomentar o debate acerca da vulnerabilidade do indíviduo na grande rede de computadores.

No que tange a proteção de dados pessoais em ambientes cibernéticos, foi possível perceber ao longo da elaboração do trabalho que falta, sobretudo, informação ao usuário médio. Esta que seria elementar no sentido de despertar consciência sobre o real intuito das aplicações gratuitas de uso massivo, progressivo e diário da população. Entretanto, a informação curiosamente é acessível e está presente em todos os termos de uso, termos e condições e diversas outras nomenclaturas aplicáveis à políticas de privacidade na internet, que em última análise são contratos que a maioria absoluta dos usuários não lê, e ainda que as lesse, tais contratos não são elaborados em uma linguagem acessível, e tampouco estaria o usuário bem amparado em si para extrair o melhor destas informações e entender realmente os meandros das

cláusulas ali presentes.

Desta forma, existe uma tremenda disparidade de armas que separam o usuário de quem controla e trata suas informações pessoais no ambiente virtual, e é possível que o cenário não seja favorável no tocante às próximas gerações.

É preciso que se pense em mecanismos de legislar e prover tutela efetiva em torno do tema, que não se baseiem em sistemas de leis pensados há mais de três décadas, para solucionar demandas inéditas. Nesse contexto, além de novos mecanismos, é necessario reavaliar a autodeterminação informacional, que desde Alan Westin firmou de forma simplista que esta exporia de forma plena a mais verdadeira vontade do indivíduo. O tempo tratou de mostrar que a teoria da autodeterminação informacional não empodera o indivíduo, mas justamente o contrário.

Além disso, o trabalho buscou jogar luz aos pontos que devem ser levados em consideração na manutenção da privacidade de dados, entre estes a teoria de *surveillence*, que em tradução pouco precisa para a língua portuguesa, representa um sistema de vigilância, onde todos vigiam todos. Este estado de vigilância, por sua vez, se mostra líquido, se opõe a ideia de controle.

Não há um ordenamento na forma com que o indivíduo é vigiado e controlado, entretanto, se há algum controle, este é exercido pelos *tiny brothers*, entes majoritariamente de direito privado que tratam os dados pessoais que circulam neste emaranhado de informações. Há sempre de se levar em consideração que todos os dias alimenta-se um desmedido banco de dados com atividades diárias, informações sensíveis, formulários, fotografias, vídeos e, enfim, a intimidade de uma sociedade em sua integralidade – por meio de *softwares* que, antes de tudo, representam um modelo de negócio.

A apresentação da hipótese de que o consentimento previsto nas leis de proteção de dados pessoais, e sobretudo na LGPD possa ser passível de vício do consentimento por parte do usuário, é comprovada por alguns pesquisadores no ramo da privacidade de dados. Nesse passo, o consentimento sofreu ao longo do tempo em que se desenvolvem leis de proteção de dados, o que pode-se definir como uso excessivo, já que desde as primeiras gerações de leis, confiou-se neste instituto, colocando-se sua função como indicativo de escolha do indivíduo em primeiro lugar.

Entretanto, as politicas de privacidade seguem inacessíveis, extensivas e complexas para delas resultarem um consentimento válido, e tais termos sejam talvez

uma medida de salvaguarda dos próprios entes que as produzem, no sentido de protegerem-se do ilícito. Assim, é possível que quanto mais específicas forem as leis nestes moldes, como a LGPD, mais longos serão os termos de uso elaborados pelas empresas, e por conseguinte, mais distância haverá entre o usuário médio desprovido de conhecimento técnico, e os contratos celebrados na internet.

É importante pontuar que, muito embora estas políticas de termos de uso sejam negligenciadas pelo usuário-médio, elas tenham seu lugar na proteção contra a responsabilidade legal, mas, sobretudo, não protegem os indivíduos como deveriam. E - ainda que assim possa se pensar, mesmo que as políticas de privacidade fossem mais curtas e mais dinâmicas, isto ainda não as fariam prover um consentimento mais válido – muito em função das práticas de *neuromarketing* e do reflexo do indivíduo em buscar o ato final de acessar a aplicação que se busca, ignorando qualquer *pop-up* que esteja no caminho. É trabalho dos estudos contemporâneos sobre o tema questionarem quais são os mecanismos que poderão solucionar o conflito entre as práticas informacionais dos dias atuais e os instrumentos jurídicos arcaicos que os enfrentam na atualidade, a fim de que estes possam estar em consonância com a tecnologia vigente, pois é possível que não se esteja legislando com a clareza necessária.

Já que o caminho que as leis traçam no sentido de depositar no usuário a responsabilidade de enfrentar, munido apenas de seu frágil consentimento, as complexidades dos termos de uso e contratos – não está livre de fraquezas. A sociedade em rede tem confiado demais na autodeterminação de dados em detrimento de outros mecanismos e ferramentas de proteção da privacidade, sobrecarregando os individuos leigos, para que se aventurem como profissionais do direito da privacidade, em cada vez mais complexos e difíceis ambientes virtuais a serem desbravados. Além disso, a sociedade em rede subestima a necessidade de adaptar os princípios de privacidade às rápidas mudanças que a tecnologia está trazendo.

Ora, se os problemas são de fato inéditos e derivados de uma tecnologia de avanço exponencial, talvez caiba ao Direito adentrar ao território tecnológico, para que exerça uma regulação com a devida paridade de armas.

Se forem empreendidos de forma adequada, novos instrumentos podem agregar valor ao consentimento, concentrando o seu uso para situações específicas, em que realmente o consentimento, livremente cedido e específico, seja o método mais adequado.

Quando não for este o caso, o trabalho árduo de pesquisadores, estudiosos, legisladores e executivos deve se dar no sentido de promover novas ferramentas que fomentem, sobretudo, práticas responsáveis, mas sem perder o foco nos indivíduos que tem seus dados pessoais tratados, a fim de dar-lhes o mais legítimo empoderamento individual livre de prejuízos.

REFERÊNCIAS

ACQUISTI, Alessandro & GROSSKLAGS, Jens**. Privacy and rationality in individual decision making. Security & Privacy**, IEEE. 3. 26 - 33. 10.1109/MSP.2005.22. (2005).

BAUMAN, Zygmunt. **Vigilância líquida,** Diálogos com David Lyon. Rio de Janeiro: Zahar, 2014.

BELLAMY, Bojana. HEYDER, Markus. **Empowering Individuals Beyond Consent.** 2015**.** Disponível em: https://www.huntonak.com/files/Uploads/Documents/Centre/Centre_Bellamy_Heyder_IAPP_Privacy_Perspective.pdf

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Bruno Ricardo Bioni. – 2. Ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil.** GPoPAI/USP grupo de pesquisa em políticas públicas para o acesso à informação. São Paulo, 2015.

BOBBIO, Norberto. **Igualdade e liberdade**. Tradução: Carlos Nelson Coutinho. 2. ed. Rio de Janeiro: Ediouro, 1997.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. / Escola Nacional de Defesa do Consumidor; elaboração **Danilo Doneda**. – Brasília: SDE/DPDC, 2010

BRASIL. **Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 30/06/2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Código de Defesa do Consumidor. 1990. Disponível em: . Acesso em: 11 ago. 2016.

BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. 2002. Disponível em: . Acesso em: 30 out. 2020.

BRASIL. **Marco Civil da Internet, Lei nº 12.965/2014**. Brasília, DF: Presidência da República, 2014. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30/06/2020.

CHADWICK, P. **How many people had their data harvested by Cambridge Analytica?** The Guardian. 19 de abr. de 2018. Disponível em: <https://www.theguardian.com/commentisfree/2018/apr/16/how-many-people-data-cambridge-analytica-facebook>. Acesso em 21/05/2020.

CONSELHO DA EUROPA, **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.** ETS Nº 108. Strasbourg, 28/01/1981.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais** [livro eletrônico] : elementos da formação da Lei Geral de Proteção de DadoS. 2. ed. São Paulo : Thomson Reuters Brasil, 2020.

ESTRADA, Manuel Martín Pino. **O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade.** *Revista de Direito do Trabalho*, v. 172, p. 43, nov./dez. 2016.

MAGRANI, Eduardo. Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. Rio de Janeiro: Arquipélago Editorial, 2019.

MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc (Org.). **Technology and Privacy: The New Landscape.** Cambridge: The MIT Press, 1997. P. 219-242.

MAYER-SCHONEBERGER, Viktor. CUKIER, Kenneth. **Big Data**: A revolution will transform how we live, work and think. New York: Houghton Miff lin Publishing, 2013.

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

PARCHEN, Charles Emmanuel. FREITAS, Cinthia Obladen de Almendra. MEIRELES, Jussara Maria Leal. "AS TÉCNICAS DE NEUROMARKETING NOS CONTRATOS ELETRÔNICOS E O VÍCIO DO CONSENTIMENTO NA ERA DIGITAL." *Novos Estudos Jurídicos* [Online], 23.2 (2018): 521-548. Web. 30 Nov. 2020
SOLOVE, Daniel. **The Digital Person: Technology and Privacy in the Information Age**, Nova York, New York University Press, 2007, p.47.

SOLOVE, Daniel. **Understanding Privacy**, Cambridge, Mass.: Harvard University Press, Copyright © 2008 by the President and Fellows of Harvard College.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Resenha à obra Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**, São Paulo: Thomson Reuters Brasil, 2019

TSOHOU, Aggeliki; KOSTA, Eleni. **Enabling valid informed consent for location tracking through privacy awareness of users: A process theory.** Computer Law & Security Review. 2017.

WESTIN, Alan F. Privacy and Freedom. New York. Atheneum, 1970.