O Laboratório de Pesquisa em Políticas Públicas e Internet é um grupo de extensão da UnB focado em realização de pesquisas na área das Ciências Sociais e a Tecnologia, além de organizar eventos e participar em debates sobre temas tais como Privacidade de Dados, Blockchain e Fake News. Atualmente, o grupo atua como amicus curiae na ADPF 403, o "Caso WhatsApp".

O CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS: ANÁLISE DO PL 4060/2012 E SUA CONJUNTURA LEGISLATIVA

THE CONSENT IN THE PROTECTION OF PERSONAL DATA: ANALYSIS OF PL 4060/2012 AND ITS LEGISLATIVE CONJUNCTURE

Alexandra Souto Maior[352]

Amanda Espiñeira[353]

Alicia Akamine[354]

Gabriel Araújo Souto[355]

Thiago Moraes[356]

Ana Cláudia Farranha[357]

RESUMO

A análise do panorama legislativo do Projeto de Lei nº 4060/2012 encontra-se imersa no avanço tecnológico e na necessidade da regulamentação do uso e da troca de dados pessoais que as relações do meio digital implicam. Neste artigo, aborda-se o estudo das múltiplas influências que impactam o PL 4060/12 e os diversos setores sociais que cobiçam por ter seu posicionamento normatizado. Desse modo, examinamos o trâmite legislativo junto às audiências públicas do PL e o embate paradigmático entre a necessidade de celeridade para a regulação do consentimento, suas características e o equilíbrio entre os polos políticos para atender aos anseios sociais.

[352] Advogada. Bacharel em Direito pela PUC-Campinas. Especialista em Direito Contratual pela PUC-SP. Pesquisadora do LAPIN/UnB.
[353] Mestranda em Direito pela UnB, bolsista CAPES. Advogada. Bacharel em Direito pela UFBA. Pesquisadora do LAPIN/UnB.
[354] Acadêmica de Direito da Universidade de Brasília. Pesquisadora do LAPIN/UnB.
[355] Acadêmico de Direito do IDP. Bolsista no ano de 2017 dos programas Youth@ForumBR e Youth@IGF do CGI.br. Intercambista do 38º Programa de Intercâmbio do Cade. Pesquisador do LAPIN/UnB.
[356] Assessor jurídico. Bacharel em Direito e Engenharia de Redes e Mestre em Ciência da Informação, pela UnB. Pesquisador do LAPIN/UnB.
[357] Professora Adjunta da Faculdade de Direito da Unb, Coordenadora do LAPIN/UnB

PALAVRAS-CHAVE: consentimento; dados pessoais; titularidade dos dados pessoais; legítimo interesse.

ABSTRACT

The analysis of the legislative landscape of the Bill 4060/2012 is immersed in the technological advance and in the necessity of regulation of the relations that the digital medium implies. Thus, this study focuses on the multiple influences that impact PL 4060/12 and the various social sectors that covet to have their positioning standardized. In this way, it examines the legislative process in the public hearings of PL 4060/12 and the paradigmatic clash between the need for speed to regulate consent and its characteristics and the balance between political poles to address social desires.

KEYWORDS: consent; personal data; ownership of personal data; legitimate interest.

1. INTRODUÇÃO

A necessidade normativa do consentimento dos dados pessoais se torna perceptível na conjuntura moderna guiada pela *data-driven economy*. O panorama comercial voltado à valoração das informações pessoais faz com que haja a confusão de direitos contratuais frente à tutela da privacidade individual. Assim, empresas multissetoriais, além de guardarem os dados dos seus clientes, podem unilateralmente usá-los para outras atividades ou até mesmo vendê-los sem o consentimento prévio do titular dos dados, fazendo-se necessária a construção protetiva de normas que regulam as relações B2C (*Business-to-Customer*) e B2B (*Business-to-Business*) a fim de evitar a imprevisibilidade de tais atitudes ilícitas.

As consequências do uso indevido de dados pessoais revela uma sociedade insegura com os meandros tecnológicos, pouco precavida e até mesmo alheia ao assunto. Segundo o *4th annual MEF Consumer Trust Study*, de 6.500 usuários de dispositivos móveis, 53% consideram que não estão no controle da maneira como seus dados são usados. Destes, 39% aderem completamente à permissão dada por meio de Termos e Condições com o sentimento de impossibilidade de escolha[358]. Face à isso, segundo o Financial Times, dados gerais sobre uma pessoa valem, no mínimo, US$ 0,0005 e crescem a partir de informações mais específicas, como a classe social e as condições de saúde do indivíduo[359].

No contexto brasileiro, a intenção normativa do consentimento prévio ganha evidência com o Projeto de Lei nº 4060 de 2012, o qual possui cláusulas gerais que tratam sobre o

[358]MOBILE ECOSYSTEM FORUM. **The 4th annual MEF Consumer Trust Study**. Disponível em: <https://mobileecosystemforum.com/programmes/consumer-trust/global-consumer-trust-survey-2017/>. Acesso em: 06 mai. 2018.
[359]FINANCIAL TIMES. **How much is your personal data worth?**. Disponível em: <https://ig.ft.com/how-much-is-your-personal-data-worth/>. Acesso em: 06 mai. 2018.

compartilhamento de dados visando a boa-fé, a lealdade e o legítimo interesse e normas que propõem o estabelecimento do consentimento do usuário, mas que não possuem um rol taxativo sobre de que forma este seria acordado e validado.

A metodologia adotada na elaboração textual consistiu na revisão bibliográfica sobre regulação dos dados pessoais e na análise das audiências públicas realizadas no âmbito do PL 4060/12. Desse modo, a partir de uma perspectiva exploratória e demonstrativa, buscou-se a classificação do posicionamento dos *players,* i.e. Sociedade Civil, Setor Privado, Comunidade Acadêmica e Setor Governamental, os quais foram identificados em cada audiência e a categorização de suas respectivas opiniões para a síntese dos conceitos e ideias presentes no artigo.

Ademais, o presente artigo busca a análise responsiva das seguintes perguntas: Quais seriam os requisitos para um modelo ideal de consentimento? e Há a possibilidade consensual entre os vários interesses do modelo *multistakeholder*? Assim, caberá à seguir a definição do consentimento do cidadão, os fatores e influências inerentes ao seu debate quanto à legitimidade para o uso dos dados pessoais, o modelo contratual virtual, o mercado econômico digital e, por fim, o consentimento no âmbito dos menores de idade.

2. O PL 4060 E O CONSENTIMENTO DO TITULAR NO PROCESSO DE EFETIVO CONTROLE DO CIDADÃO SOBRE SUAS PRÓPRIAS INFORMAÇÕES

Em uma sociedade da informação, os dados pessoais estão sendo constantemente coletados, armazenados e processados para atender diversas finalidades (MURRAY, 2016). Os benefícios advindos com essa prática são evidentes, como a criação de produtos e serviços que atendem demandas específicas dos consumidores.

O potencial de coleta, processamento e utilização dos dados pessoais é aumentado consideravelmente diante do avanço da tecnologia da informação. E os dados coletados indicam as localizações por onde a pessoa passa, os gostos, os padrões de consumo, informações essas que cruzadas traçam perfis refinados que possibilitam o desenvolvimento da Internet das Coisas e de outras tecnologias. Diante desses novos fenômenos e dos interesses múltiplos nos dados pessoais, começam a ser elaboradas regulações de comportamentos e direitos, a fim de proteger essas informações. Assim, as repercussões dos modelos regulatórios de proteção dos dados pessoais afetam diretamente o processo econômico e as relações comerciais contemporâneas. Nesse sentido, a importância da proteção à privacidade vem à tona no mundo e o Brasil não está fora desse contexto, em que cerca de 109 países possuem legislação sobre o tema.

Desse modo, tendo em vista que o tratamento de dados pessoais precisa obedecer a parâmetros bem definidos, a fim de não violar o direito fundamental do indivíduo à privacidade (MENDES, 2014), foi elaborado o Projeto de Lei nº 4060/2012 (PL 4060/2012), ao qual foi apensado o Projeto de Lei nº 5276/2016 (PL 5276/2016).

2.1. Breve panorama do PL de dados pessoais: definindo os contornos do debate

O texto do anteprojeto do PL 5276/2016 foi elaborado pelo Executivo e passou por um debate público promovido pelo Ministério da Justiça e pelo Centro de Estudos sobre Tecnologias Web (Ceweb), vinculado ao Núcleo de Informação e Coordenação do Ponto BR (Nic.br) do Comitê Gestor da Internet (CGI), além do Instituto Nacional de Ciência e Tecnologia para a Web (InWeb), da Universidade Federal de Minas Gerais (UFMG), cuja discussão no Poder Executivo com as contribuições do debate, levaram ao texto final, agora passível de discussões no Legislativo, inclusive com a realização de audiências públicas para debater o tema na Câmara dos Deputados.

O PL, portanto, almeja estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, como a limitação a uma finalidade específica, a criação de um ambiente seguro e controlado para seu uso. Visa assegurar, também, o controle e a titularidade das informações pessoais. O texto apresentado possui um caráter mais robusto e elaborado sobre o tratamento de dados, por ter contado com o auxílio de especialistas e estudiosos sobre o tema, além de ter passado por um amplo debate prévio ao PL.

Então, por uma questão temporal, ao ser apresentado ao Congresso Nacional, foi apensado ao PL 4060/2012 na Câmara dos Deputados. Na tramitação deste PL foram realizadas audiência públicas com representantes da Sociedade Civil, da Comunidade Acadêmica, do Setor Privado e do Governo, para ampliar o debate e aprimorar a futura lei. Nessas audiências foi discutida a importância de uma definição e conceituação de dados pessoais, sensíveis, anônimos, entre outros, para delimitar a aplicação da lei.

O modelo regulatório a ser adotado, também foi abordado nas audiências. Após análise, foram levantadas as principais teses apresentadas pelos atores participantes que apontaram alguns elementos para a construção do modelo regulatório brasileiro. A primeira delas é que empresas estatais devem obedecer às mesmas regras de proteção de dados que as empresas privadas. Ademais, o conceito de dados sensíveis deve ser mais restrito, isto é, devem se restringir aos dados identificados, não os identificáveis. Além disso, os dados identificáveis não devem possuir todas as informações sobre um usuário. O consentimento do usuário é importante, mas pode ser limitado por regras legais e contratuais. Assim, a

legislação não pode criar barreiras para a utilização dos dados pessoais.

Sugere-se que o PL tenha uma *vacatio legis* de 3 anos. Outrossim, a regra de transição não deve se sujeitar a regulação futura. Também não pode haver responsabilidade solidária entre cedente e cessionário. Devem haver normas premiais que estimulem condutas de proteção de dados por empresas e usuários. Além disso, o PL não pode ser exageradamente minucioso e deve focar em conceitos abertos.

Ressalta-se que as definições de privacidade variam de acordo com o contexto em que se insere, com o modelo regulatório adotado por cada país diante de elementos vários. A privacidade é, portanto, "uma pluralidade, cuja busca por uma essência única está fadada ao fracasso"[360] (SOLOVE, 2008, p.3). Entretanto, a proteção legal da privacidade depende do conceito que informa o objeto dessa proteção, sua natureza e seu escopo. Assim, compreende-se o prisma da complexidade que envolve a privacidade.

Definir e delimitar a privacidade são tarefas complexas pelo fato de estarem ligadas aos valores e projeções do homem em cada sociedade. Contudo, apesar de a forma como a proteção à privacidade é implementada depender das diferentes jurisdições e de diversos atores sociais, como o mercado e outros reguladores que influenciam esse processo, "a necessidade de buscar um mínimo conteúdo comum para o direito à privacidade, é mais que um exercício puramente acadêmico, antes uma necessidade real diante do incremento no fluxo de informações nos últimos anos". (DONEDA, 2006, pp.85-86)

A ressignificação dos dados e os valores que eles passam a ter diante das mudanças tecnológicas e sociais leva os países a se adaptarem a essa nova realidade diante de necessidades primordialmente econômicas, dentre outras interações necessárias no mundo conectado. A construção de modelos regulatórios de tratamento e proteção dos dados pessoais passa a ser essencial e a definição de privacidade é fundamental quando as informações pessoais atingem a esfera política. (BAMBERGER, 2013). Assim, a privacidade assume posição de destaque na proteção da pessoa humana como elemento indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade (DONEDA, 2006; SOLOVE, 2008).

A proteção de dados pessoais, nesse contexto, também retoma a proteção da dignidade da pessoa humana em que os direitos da personalidade são direitos fundamentais, inclusive no art. 12 da Declaração Universal dos Direitos Humanos[361]. A superação do direito à

[360] Tradução própria do original em inglês: "[…] privacy is a plurality of different things and that the quest for a singular essence of privacy leads to a dead end".

[361] Artigo 12. Ninguém será sujeito à interferências em sua vida privada, em sua família, em seu lar ou em sua

privacidade como uma tutela de índole apenas patrimonial, diante desse cenário em que é encarado como um direito fundamental, e o estabelecimento de novos mecanismos e institutos para possibilitar a efetiva tutela dos interesses da pessoa, isto é, a funcionalização da proteção da privacidade fez, portanto, com que dela surgisse uma disciplina de proteção de dados pessoais.

Não obstante, depender de fatores subjetivos tais quais o tempo e o local, a privacidade não deve ser encarada como um direito subjetivo. Um dos motivos para tanto é a própria dificuldade em enquadrarmos a privacidade em uma concepção coerente e unitária. (DONEDA, 2006) Antes, deve ser vista como uma situação subjetiva complexa, cuja tutela depende do sopesamento de situações concretas de sua aplicabilidade, a qual na definição de Pietro Perlingieri (1982) "[...] se expressa através do exercício arbitrário do poder pelo seu titular, porém influi outros interesses, tanto do titular quanto da coletividade, que implica em poderes, deveres, obrigações e ônus aos envolvidos". (p.279)

Importante, ainda, apontar como um elemento nesse debate, o "consentimento", enquanto legitimação do titular dos dados ao tratamento dos mesmos. Nesse sentido, nota-se que o debate é mais amplo e complexo, já que "a percepção da população na necessidade de se estabelecer um mecanismo de proteção de dados implica no atendimento de outras necessidades básicas como o padrão médio de consumo, a educação, a penetração da tecnologia no cotidiano e o próprio acesso à rede". (DONEDA, 2006, p.17)

2.2. Legitimidade para o uso dos dados pessoais: relevância do consentimento na proteção

Dentre os temas abordados nas audiências públicas da PL 4060/2012, destaca-se o do consentimento, pois é uma das formas de legitimar o tratamento dos dados pessoais[362], além de possibilitar o controle do indivíduo sobre seus dados com o exercício da autodeterminação informativa.

O ordenamento jurídico brasileiro contempla a proteção da pessoa humana como seu valor máximo e a privacidade como um direito fundamental assegurado pela Constituição no art. 5º, X e XII[363]. Há ainda proteções fracionadas com focos de atuação determinados, tal

correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

[362] Há outras formas de obter acesso aos dados pessoais de modo legítimo, como ocorre quando o responsável pelo tratamento dos dados possui interesse legítimo. Essa hipótese está presente, inclusive, no artigo 7º, inciso IX, do PL 5276/2016.

[363] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das

qual o art. 43 do Código de Defesa do Consumidor e na Lei de Cadastro Positivo (Lei nº 12.414/2011), em que se regula basicamente banco de dados sobre consumidores.

Além disso, a privacidade dos dados pessoais está presente nos arts. 4º[364] e 31[365] da Lei de Acesso à Informação (LAI), que será melhor discutida no tratamento dos dados pelo Poder Público. Há também previsão do tema em dispositivos no Marco Civil da Internet, destacando-se a proteção da privacidade e dos dados pessoais como um princípio para o uso da Internet, no art. 3º[366], bem como um direito assegurado no uso da rede, considerado essencial ao exercício da cidadania, no art. 7º[367], além de parte dos arts. 10[368] e 11[369] que se inserem na Seção "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações

---

pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...] 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.

[364] Art. 4º Para os efeitos desta Lei, considera-se: I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato; III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; VI - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados; VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema; VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

[365] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

[366] Art. 3° A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei. [...] Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

[367] 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; [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei.

[368] 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.

[369] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Privadas". A tutela da privacidade, todavia "depende de uma valoração complexa na qual sejam sopesadas situações concretas de sua aplicabilidade" (DONEDA, 2006, p.17), sendo o PL de dados pessoais um ambiente propício para que este modelo regulatório seja desenvolvido no Brasil. Essa abrangência não permite, portanto, uma categorização da lei como pública ou privada, por sua efetividade envolver a aplicação à diversos ramos jurídicos. (KUNER, 2010)

Dessa forma, as definições de privacidade variam de acordo com o contexto em que se insere, com o modelo regulatório adotado por cada país, delimitados por valores, normas sociais e interesses. Assim, enquanto a UE tem uma regulação proativa sobre os dados pessoais, os EUA tem a auto regulação do mercado como modelo para o tema. (FERNBACK; PAPACHARISSI, 2007)

O modelo europeu de regulação da privacidade até então baseado na Diretiva 95/46, será substituído em maio de 2018 pela *General Data Protection Regulation* (GDPR), aprovada em abril de 2016, e elaborada com a finalidade de harmonizar as leis de privacidade de dados, proteger e empoderar a privacidade de dados dos cidadãos da UE, bem como para remodelar a forma como as organizações abordam a privacidade de dados. Este modelo considera privacidade como um direito fundamental, cuja responsabilidade de assegurar aos cidadãos é do governo. Direito esse que é reproduzido em diversas constituições de países na Europa e no art. 8º da Convenção do Conselho europeu para proteção dos direitos humanos e liberdades fundamentais[370]. (MOVIUS; KRUP, 2009; KUNER, 2010)

De acordo com o artigo 4 (11) do regulamento europeu (GDPR), o consentimento somente será válido se for dado de forma livre, específica, informada e inequívoca. Entende-se que o indivíduo que não é coagido a consentir, o faz de forma livre. Por sua vez, se ele compreende o que irá acontecer com os seus dados, permite seu uso para uma determinada finalidade e expressa sua permissão sem ter dúvidas, ele está consentindo de modo específico, informado e inequívoco, respectivamente[371].

Acrescenta-se, também, aos requisitos de validade do consentimento, a necessidade de ser revogável pelo titular dos dados pessoais. Afinal, o pleno exercício da autodeterminação

[370] ARTIGO 8° Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

[371] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on consent under Regulation 2016/679**. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 05 mai. 2018.

informativa, permite ao usuário deixar de concordar com a utilização dos seus dados, caso entenda que não está mais sendo beneficiado com o processamento.

Compreendida a importância do consentimento do titular para a privacidade e proteção dos dados pessoais, no próximo tópico será feita a análise dos argumentos proferidos na Audiência Pública sobre consentimento no âmbito do PL 4060/2012, a fim de expor e compreender as preocupações e demandas dos representantes do Setor Privado, Comunidade Acadêmica, Sociedade Civil e Governo brasileiro sobre o tema.

3. MODELO REGULATÓRIO PARTICIPATIVO: ANÁLISE DOS ARGUMENTOS DA AUDIÊNCIA PÚBLICA SOBRE CONSENTIMENTO NO PL 4060

3.1. Termos de uso e consentimento

A validade dos contratos eletrônicos já é tema pacificado na jurisprudência brasileira, e tratado em âmbito internacional pelas discussões da lei modelo sobre o comércio eletrônico da Comissão de Direito do Comércio Internacional da Organização das Nações Unidas – UNCITRAL – de 1996, a qual regula o comércio eletrônico em geral, bem como sua aplicação em atividades específicas.

Comércio eletrônico é a venda de produtos (virtuais ou físicos) ou a prestação de serviços realizadas em estabelecimento virtual. A oferta e o contrato são feitos por transmissão e recepção eletrônica de dados. O comércio eletrônico pode realizar-se através da rede mundial de computadores ou fora dela. (COELHO, 2007, p. 32)

Os contratos de adesão são aqueles por meio dos quais diversas pessoas podem aderir ao mesmo bloco de condições gerais propostas por uma das partes, de modo que não contêm a regulação para um caso específico, e sim para uma generalidade de diversas contratações. Nessa modalidade, a parte que adere, ou seja, que aceita as condições gerais propostas, é submissa ao que lhe for imposto através dessas condições.

Importante destacar a diferença entre as cláusulas gerais do ordenamento jurídico e as cláusulas gerais dos contratos de adesão, conforme ensina o Ministro Ruy Rosado de Aguiar Jr.:

> A cláusula geral do Direito é uma norma jurídica que serve para avaliar a conduta, mas não define essa conduta. É norma em branco que atribui ao aplicador a função de estabelecer, caso a caso, qual a conduta devida, isto é, qual o comportamento esperado do cidadão, naquelas circunstâncias e naquela relação.[...]O nosso sistema jurídico contém inúmeras cláusulas gerais (que não se confundem com as cláusulas gerais do negócio, portanto estas são apenas cláusulas contratuais pré ordenadas pelo estipulador e vão

> integrar o contrato de adesão, onde também são chamadas de condições gerais, cláusulas uniformes, etc.). As cláusulas gerais do ordenamento jurídico são janelas abertas no sistema, que servem tanto para a elaboração de preceitos jurídicos, de outro modo dificilmente alcançáveis, como para a inserção de fatores nele ausentes, inclusive metajurídicos. (AGUIAR JÚNIOR, 1994, p. 28)

A contratação de adesão possui como vantagem a fácil utilização para contratos de massa, e por isso simplifica a atividade empresarial. Entretanto, sua utilização facilita vantagens unilaterais e abusivas para o fornecedor que é a parte propositora das condições.

A dinâmica das contratações por meio da Internet é propícia a essa modalidade de contratação, que costuma ocorrer através de apenas um clique, eis que basta o aceite do cliente sobre as condições gerais que lhe são propostas para que a relação jurídica se efetive. O momento exato da celebração do contrato, nessas hipóteses, é aquele em que o consumidor efetivamente recebe o aviso de recebimento de sua aceitação.

Como modalidade particular de contratos de adesão, no campo da contratação eletrônica, impende destacar as chamadas licenças "*clickwrap*" ("*clickwrap agreements*" ou "*point-and-click agreements*"), usualmente submetidas à concordância do usuário do produto ou serviço, contendo cláusulas acerca de sua prestação, sendo assim denominadas, pois sua validade se baseia no ato de apertar o botão de aceitação.(MARTINS, 2016, p. 131)

Na atual sociedade da informação não se pode prescindir dos serviços contratados por meio da Internet, por isso se questiona se o consumidor teria a efetiva possibilidade de não aceitar as condições impostas pelos fornecedores.

O valor de alguns produtos ou serviços tem variação dependendo da quantidade de usuários. O usuário depende da interação com outros usuários para que tal produto ou serviço lhe seja útil, o que configura o denominado efeito de rede.

Ademais, a influência das redes baseadas na Internet vai além do número de seus usuários: diz respeito também à qualidade do uso. Atividades econômicas, sociais, políticas, e culturais essenciais por todo o planeta estão sendo estruturadas pela Internet e em torno dela, como por outras redes de computadores. De fato, ser excluído dessas redes é sofrer uma das formas mais danosas de exclusão em nossa economia e em nossa cultura. (CASTELLS, 2003, p. 8)

Quanto mais essencial o serviço se torna, qual a possibilidade que o cidadão terá de se recusar a consumi-lo? Ainda mais se considerado o fato de que essa recusa o tornará à

margem da própria sociedade em que deveria ser inserido.

Acredita-se que muitos serviços, como de correio eletrônico, mensagens instantâneas, redes sociais, programas de fidelidade, etc., sejam gratuitos. Porém, trata-se em verdade de uma compra efetuada pelo consumidor, por meio de uma remuneração indireta, concretizada ao aceitar os contratos de adesão denominados termos e condições de uso. E nessa negociação a moeda de troca é a informação.

As redes sociais demonstram mais claramente esse fornecimento de informações de forma espontânea e consciente, como por exemplo o compartilhamento de informações íntimas, fotografias e exposição de relacionamentos. Entretanto, as informações fornecidas vão além daquelas que os usuários fazem espontaneamente.

Com a aceitação dos termos e condições de uso, os consumidores divulgam dados como suas localizações geográficas, listas de contatos, suas preferências de pesquisa em sites motores de busca e até liberam acesso à câmera dos smartphones.

Tendo em vista, portanto, o valor econômico do capital social das redes e, assim, das informações que constituem as interações entre os perfis, já não há mais que se falar em gratuidade das relações jurídicas entre os sites e seus membros, usuários e, portanto, consumidores dos serviços oferecidos (MARTINS, 2016, p. 54), mediante remuneração indireta. A remuneração é indireta posto que as informações fornecidas são monetizadas pelos fornecedores.

A relação enquadra-se, portanto, no conceito de serviço (art. 3º, parágrafo 2º, da Lei 8078/90[372]), e constitui verdadeiro negócio jurídico oneroso.

> Para possibilitar o controle do titular acerca dos seus dados, outro princípio relevante é o princípio do consentimento. [...] Segundo esse princípio, o consentimento deve ser livre, específico e informado, e apenas situações excepcionais (previstas legalmente) justificam o processamento de dados sem o prévio consentimento do titular.(MENDES, 2014, p. 71)

Esse consentimento, atualmente, é extremamente discutível, dado o caráter essencial de utilização dos serviços oferecidos na Internet, bem como a falta de ciência quanto à destinação final dos dados pessoais.

O Estado deve se adequar às revoluções tecnológicas que transformam a sociedade, e

[372] Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
§ 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

regular até mesmo as relações privadas, de forma que seja garantida a função social do contrato e consequentemente a proteção dos direitos fundamentais do ser humano em relação aos modelos de negócio atuais.

3.2. Consentimento para o mercado digital: convergência quanto à releviancia, discordância quanto às suas características

Na análise dos discursos proferidos nas audiências públicas da PL nº 5.276/2016, verificou-se que os atores da Sociedade Civil, da Comunidade Acadêmica, do Setor Privado e do Governo concordaram que o consentimento do titular dos dados pessoais é essencial para a realização do tratamento de dados pessoais. Contudo, as propostas apresentadas para definir de que forma esse consentimento se daria divergiram.

Representantes da Sociedade Civil defenderam a importância de que este consentimento seja inequívoco, ou seja, o indivíduo deve consentir de forma espontânea e informada acerca da finalidade do processamento dos seus dados pelo serviço ou plataforma de tecnologia a que se vincula. Destacou ainda que deveria ser possível revisar ou revogar este consentimento, visto que ele é uma concessão precária.

Estes argumentos foram aceitos em parte pelos representantes do Setor Privado, que apresentaram uma ressalva: a dificuldade de se identificar, na prática, todas as possíveis situações em que os dados do usuário seriam tratados, o que leva muitas plataformas a optarem por adotar um modelo de consentimento genérico. Defenderam que este tipo de concessão, mais ampla, poderia ser eventualmente restringida por previsões legais ou contratuais.

Considerando o atual texto do PL 5.276/2016, o consentimento genérico seria vedado, pois ele deve ser específico, ou seja, os dados pessoais que sejam alvo do tratamento devem ter seu destino devidamente detalhado para o titular. Como isto impactará os modelos de negócio dos serviços de tecnologia é algo ainda a ser observado.

Quanto à forma do consentimento, o modelo brasileiro é um pouco mais restritivo do que a versão européia. Na GDPR, conforme o art. 7º, qualquer forma pode ser utilizada, desde que permita ao controlador de dados provar que o consentimento foi dado. Já a regra prevista na PL, exige que o consentimento seja dado pela forma escrita, ou outro meio que permita sua certificação.

Outras características importantes do consentimento, que estão previstas tanto na GDPR quanto no texto atual do PL é que este deverá ser livre, ou seja, deve se dar sem nenhum tipo de pressão ou coação sobre o titular dos dados; expresso - a pessoa deve

apresentar uma indicação clara e objetiva de que concorda que seus dados sejam tratados e com as implicações decorrentes; e informado - o titular deve ter a ciência sobre o que é o tratamento de dados pessoais e as implicações do tratamento.

Fica-se a dúvida se estas novas previsões normativas quanto ao consentimento extinguirão os contratos do tipo *click-wrap*, em que o consumidor clica em uma caixa de diálogo após uma extensa lista de termos de serviço, aceitando que seus dados pessoais sejam utilizados pela plataforma de tecnologia.

3.3. Legítimo interesse

Uma das previsões de grande polêmica no debate do consentimento é a questão do legítimo interesse, prevista no inciso IX, do art. 7º, do texto atual da PL 5.276/2016:

> Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> (...)
>
> IX - quando necessário para atender aos **interesses legítimos** do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade. (grifos acrescidos)

O receio aqui é que esta previsão crie uma exceção que abra caminho para abusos por parte daqueles que tratam dados pessoais. Em entrevista ao InternetLAB[373], o grupo Intervozes, ator da Sociedade Civil, destaca que esta regra poderia ser utilizada por um controlador para tratar dados do usuário sem seu consentimento expresso, sob a alegação de que faz isso para o bem daquele indivíduo. Como exemplo, cita a hipótese do uso de dados bancários de clientes, pelas próprias instituições bancárias, para coibir fraudes, sem o consentimento inequívoco.

Já o Google Brasil e a Serasa Experian, atores do Setor Privado, defendem que esta regra ajuda a otimizar a regra de consentimento, dando uma autorização legal para o controlador de dados naquelas situações em que o tratamento está diretamente alinhado com as expectativas do usuário. Assim, essa previsão seria mais realista ao contexto de tratamento

[373] INTERNETLAB. O que pode autorizar o tratamento de dados pessoais? Disponível em: <http://www.internetlab.org.br/pt/opiniao/especial-o-que-pode-autorizar-o-tratamento-de-dados-pessoais/>. Acesso em: 7 mai. 2018.

de dados em larga escala (*big data*), sem retirar o ônus do responsável de demonstrar que está fazendo uso da hipótese de legítimo interesse de modo adequado.

Para o Instituto Brasiliense de Direito Público - IDP, ator da Comunidade Acadêmica, a previsão deste dispositivo visa um balanceamento de interesses, apresentando exceção ao legítimo interesse no caso de "prevalecerem os direitos e liberdades fundamentais do titular". Além disso, destaca que o artigo 10 do PL prevê três requisitos para o tratamento baseado no legítimo interesse, quais sejam: i) a adoção de medidas para garantir a transparência do tratamento baseado nessa hipótese e a possibilidade de o titular manifestar oposição ao tratamento; ii) a estrita necessidade como critério de legitimidade do tratamento de dados baseado nesse requisito e a necessidade de anonimização quando possível; iii) possibilidade da autoridade requisitar impacto de privacidade.

3.4. Consentimento de menores

Embora um tema pouco debatido nas audiências da Câmara dos Deputados, a questão do consentimento por menores de idade é de importante relevância para o mercado digital. Tanto a GDPR quanto o PL 5276/2016 preveem regras sobre este tema. Conforme a regulação europeia, a autorização parental é necessária para menores de 16 anos.

Já o projeto de lei brasileiro, trouxe inicialmente uma regra que permitia que menores entre 12 e 18 anos, pudesse fornecer consentimento diretamente, ressalvada a possibilidade de revogação pelos responsáveis legais. Esta regra sofreu inúmeras críticas, e atualmente, o texto tramitando no congresso apenas diz que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente". Infelizmente, o ECA não traz nenhuma regra específica sobre o tema, o que acabará impondo aos magistrados, intérpretes da lei, a conclusão sobre em que situações este consentimento poderá ser direto, ou dependerá da autorização dos pais ou responsáveis.

Uma das principais dúvidas do mercado, que não é respondida nem pela diretiva europeia nem pelo projeto de lei brasileiro é quanto à operacionalização deste consentimento. O nome dos pais passará a constar nos termos de consentimento? Haverão regras distintas para os menores incapazes absolutos e os relativos? São mais incógnitas que só serão respondidas com a atuação judicial no caso concreto.

4. CONSIDERAÇÕES FINAIS

Tendo em vista a era da informação em que a sociedade se situa, a essencialidade das contratações através da Internet já é um fato inquestionável. Em que pesem as diversas visões

interpretativas sobre o desenvolvimento social, a Internet se configura como excessivamente influente e importante fator determinante da própria sociedade, mas para isso o seu uso deve ser consciente e transparente.

A massificação das relações comerciais, constatada através da constante contratação por meio de termos de adesão e aceitação às condições gerais impostas pelos fornecedores da Internet, impede a efetivação dessa consciência e transparência.

O efeito de rede e a crescente imposição social de uso das novas tecnologias trouxeram efeitos significativos para o mundo jurídico. As contratações ocorrem de forma veloz, através de um ou poucos cliques. Os denominados termos de adesão são utilizados como meio eficaz de contratação eletrônica, possibilitando diversos novos negócios, formas de comunicação, de aprendizado, de disseminação de informação, etc. Entretanto, na mesma medida em que tais termos de adesão aceitos mediante um clique possibilitam diversos avanços, trazem à tona riscos aos direitos fundamentais do ser humano, apresentados de forma nunca antes imaginada.

Frente ao panorama global em que as normas de proteção de dados se encontram, o Brasil assume uma posição defasada que tende a agravar as relações de consumo, visto a proporção que esta tende a assumir nos próximos anos, como é demonstrado pelo estudo *Global Cloud Index* realizado pela *Visual Networking Index* que prevê com que 4 bilhões de pessoas até 2020 tenham acesso à internet[374].

Pode haver a impressão de que não existiria como alterar a relação da sociedade com os meios digitais, devido à sua imensa complexidade (multiplicidade de atores, Estados, legislações e composição geográfica distribuída), os avanços e transformações já ocorridos e à falta de regulação unificada. Porém, existem instrumentos para efetivar a proteção mínima aos direitos fundamentais. Tais instrumentos se constituem como a defesa da legislação já existente, especialmente o Código de Defesa do Consumidor, que se faz tão necessária e atual aos problemas advindos das novas realidades, bem como a criação de legislação específica.

A privacidade se constitui como direito fundamental protegido constitucional e legalmente, mas constantemente em risco nos meios digitais. Urge-se, portanto, a celeridade do processo normativo em detrimento do efeito que a necessidade do consentimento do titular dos dados causa no cenário econômico e social. Além da regulação interna de cada país, o papel dos fóruns híbridos se faz essencial para a unificação de políticas de governança da

[374]VISUAL NETWORKING INDEX. **7th annual Global Cloud Index**. Disponível em: <https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html>. Acesso em: 06 mai. 2018.

Internet, tanto na esfera pública quanto na privada.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUIAR JÚNIOR, Ruy Rosado de. Cláusulas Abusivas no Código do Consumidor - Em: *Estudos sobre a proteção do consumidor no Brasil e no MERCOSUL/Instituto Brasileiro de Política e Direito do Consumidor.* Porto Alegre: Livraria do Advogado, 1994.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on consent under Regulation 2016/679*. Disponível em: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>. Acesso em: 05 mai. 2018.

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. *The George Washington Law Review*, 81(5), p. 1529-1664, 2013.

BRASIL. *Constituição da República Federativa do Brasil de 1988.* Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 de jul. 2017.

_____. *Lei nº 12.527/2011 (Lei de Acesso à Informação*, de 18 de novembro de 2011. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 03 de jul. 2017.

_____. *Lei nº 12.965/2014 (Marco Civil da Internet)*, de 23 de abril de 2014. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 de jul. 2017.

_____. *Lei nº* (*Código de Defesa do Consumidor)*, de 11 de setembro de 1990. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 03 de jul. 2017.

CASTELLS, M. *A galáxia da Internet: reflexões sobre a Internet, negócios e a sociedade.* Traduzido por Maria Luiza X. de A. Borges. Rio de Janeiro: Jorge Zahar Ed., 2003.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FERNBACK, Jan; PAPACHARISSI, Zizi. Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. *New Media & Society*, 9(5), p. 715–734, 2007.

KUNER, Christopher. Data protection law and international jurisdiction on the Internet

(part 1). *International Journal of Law and Information Technology*, vol. 18. n. 2, p. 176 - 193, 2010.

MARTINS, Guilherme Magalhães Martins. *Contratos Eletrônicos de Consumo.* 3. ed. São Paulo: Atlas, 2016.

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

MOVIUS, Lauren B.; KRUP, Nathalie. U.S. and EU Privacy Policy: Comparison of

Regulatory Approaches. *International Journal of Communication*, 3, p. 169-187, 2009.

MURRAY, Andrew. *Information Technology Law*: Law and Society. Oxford: Oxford University Press, 2016.

ONU. *Declaração Universal dos Direitos Humanos*. Disponível em <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 10 de jul. 2017.

PERLINGIERI, Pietro. *La personalitá umana nell'ordinamento giuridico*. Napoli: ESI, 1982.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

UE. *Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais*, de 04 de novembro de 1950. Disponível em <http://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em 7 de jul. de 2017.

_____. *Diretiva 95/46/CE*, de 24 de Outubro de 1995. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 20 de jun. de 2017.

_____. *General Data Protection Regulation*. Disponível em <http://www.eugdpr.org/eugdpr.org.html>. Acesso em: 04 de jul. de 2017.