UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

O CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET:

UMA ANÁLISE COMPARADA DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU E DO PROJETO DE LEI 5.276/2016

LUÍZA FERNANDES MALHEIRO

BRASÍLIA- DF
2017

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

O CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET:

UMA ANÁLISE COMPARADA DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU E DO PROJETO DE LEI 5.276/2016

AUTOR: LUÍZA FERNANDES MALHEIRO

ORIENTADOR: ALEXANDRE KEHRIG VERONSE AGUIAR

MONOGRAFIA APRESENTADA COMO REQUISITO PARCIAL À OBTENÇÃO DO GRAU DE BACHAREL PELA FACULDADE DE DIREITO DA UNIVERSIDADE DE BRASÍLIA – UNB.

BRASÍLIA- DF
2017

Malheiro, Luíza Fernandes.

O consentimento na proteção de dados pessoais na Internet: uma análise comparada do Regulamento Geral de Proteção de Dados europeu e do Projeto de Lei 5.276/2016 / Luíza Fernandes Malheiro – Brasília/DF, 2017.

86 folhas. Monografia (graduação) – Universidade de Brasília, Faculdade de Direito, 2017. Orientador: Alexandre Kehrig Veronese Aguiar.

1.Proteção de dados, 2. Consentimento, 3. Regulamento Geral de Proteção de Dados (RGPD), 4. Regulamento (UE) 2016/679; 5. Projeto de Lei 5.276/2016.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

O CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET:

UMA ANÁLISE COMPARADA DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU E DO PROJETO DE LEI 5.276/2016

LUÍZA FERNANDES MALHEIRO

MONOGRAFIA APRESENTADA COMO REQUISITO PARCIAL À OBTENÇÃO DO GRAU DE BACHAREL PELA FACULDADE DE DIREITO DA UNIVERSIDADE DE BRASÍLIA – UNB.

APROVADA POR:

BANCA EXAMINADORA

_____
PROF. DR. ALEXANDRE KEHRIG VERONSE AGUIAR
ORIENTADOR

_____
PROF. LUANA BORGES

_____
PROF. CLARISSA VAZ MASILI

BRASÍLIA- DF
2017

AGRADECIMENTOS

Em primeiro lugar, agradeço ao Deus soberano pelo resgate, graça e sustento até aqui. O SENHOR é de fato misericordioso e compassivo, longânimo e assaz benigno.

Agradeço aos meus pais por toda paciência, apoio e dedicação ao longo desses anos. Ao meu pai, pela proteção e provisão, sempre constantes. E em especial, à grande Maria Lúcia, felizmente a minha mãe. É impossível imaginar minha trajetória sem o seu suporte, insistência, incentivo e constância. Sem as suas verdades também.

Agradeço à Universidade de Brasília, que me tirou da zona de conforto e permitiu o meu desenvolvimento acadêmico.

Aos companheiros de graduação, verdadeiros oásis e presentes ao longo da caminhada, com quem eu pude compartilhar incertezas e alegrias. Às amigas e amigos, pelo companheirismo, encorajamento, motivação e palavras certas.

Agradeço ao meu orientador, professor Alexandre Veronese, presente no decorrer da graduação, fosse nas aulas ou nos projetos de pesquisa, sempre muito acessível e com compromisso admirável com a academia. Agradeço pela orientação e conselhos, pelas boas indicações e empréstimos de bibliografia, por todo apoio.

Agradeço, por fim, à Luana e à Clarissa, que foram tão solícitas diante do meu convite. Obrigada pela dedicação de vocês, que de maneira tão motivada e didática no decorrer das aulas desse semestre, juntamente com o professor Veronese, despertaram meu gosto para o tema deste trabalho.

RESUMO

O presente estudo faz uma análise acerca da proteção de dados pessoais frente às transformações tecnológicas que levaram a uma nova configuração econômica e social, pautada na informação. Diante de um cenário em que os dados possuem valor econômico e o imperativo dos novos negócios da vigilância visa a captação dos dados pessoais, o consentimento figura como uma forma de o usuário manter-se informado e autorizar ou não a coleta, processamento e compartilhamento de seus dados pessoais na rede. Nesse sentido, é desenvolvido o papel do consentimento dentro do contexto da proteção de dados pessoais à luz da autodeterminação informativa e como um instrumento de legitimação do tratamento de dados. Para tanto, são abordados seus pressupostos de validade, sua natureza jurídica e possibilidade de revogação. O trabalho também apresenta as recentes críticas ao consentimento, bem como suas dificuldades e desafios. Por fim, faz-se uma análise comparada sobre como o Regulamento Geral de Proteção de Dados (RGPD) europeu e o Projeto de Lei brasileiro 5.276/16 sobre proteção de dados pessoais abordam a temática do consentimento.

PALAVRAS-CHAVE: Proteção de dados; Consentimento; Regulamento Geral de Proteção de Dados (RGPD); Regulamento (UE) 2016/679; Projeto de Lei 5.276/2016.

ABSTRACT

The current study analyzes the personal data protection before the last technological changes that have led to a new economic and social configuration based on information. Faced a scenario in which data has economic value and the imperative of the new surveillance is aimed at the capture of personal data, consent figures as a way to keep the user informed and able to authorize or not the personal data collection, processing and sharing on the network. In this regard, the role of consent is developed within the context of the personal data protection in the light of informational self-determination and as an instrument to legitimate the data processing. For this study proposal about consent, its validity, its legal nature and revocation possibility are addressed. The research paper also presents late criticisms on the matter of consent, as its recent difficulties and challenges. Finally, a comparative analysis is made on how the General Data Protection Regulation and the Brazilian Data Protection Bill 5276/16 on personal data protection address the subject of consent.

KEYWORDS: Data Protection; Consent; General Data Protection Regulation (GDPR); Regulation (UE) 2016/679; Brazilian Data Protection Bill 5.276/2016.

SUMÁRIO

INTRODUÇÃO

As revoluções das tecnologias da informação e comunicação nas últimas décadas foram responsáveis por alterar a sociedade a ponto de hoje ela ser reconhecida como sociedade da informação. Com o fortalecimento das redes e a ubiquidade dos meios informáticos, os dados pessoais tornaram-se um novo recurso de base nessa nova economia informacional.

Considerados a nova *commodity* e o novo petróleo do século XXI, os dados pessoais são gerados diariamente e em larga escala pelas atividades dos usuários, que passaram a ser considerados um grande centro de produção de riquezas nessa *data-driven society*. Tamanha tem sido a geração e circulação de dados que Big Data é o termo mais utilizado atualmente, referindo-se ao grande volume de dados amplamente analisados, agregados e cruzados por algoritmos de computador.

No atual modelo de negócios, as empresas oferecem serviços "gratuitamente" quando na verdade os usuários pagam em forma de dados pessoais, dados estes que são compartilhados com terceiros, movimentando um comércio de bilhões de dólares por ano. Como o dado pessoal é o novo recurso de base, a vigilância e o monitoramento sobre os usuários e a captação de seus dados são estratégias adotadas para essa nova forma de produção.

Se antes a preocupação era da figura do Estado como o Big Brother, hoje a discussão abrange também o setor privado, que utiliza massivamente os dados pessoais para atingir seus objetivos econômicos, na figura de "pequenos irmãos". Nesse cenário, as técnicas dos atuais negócios da vigilância trazem consigo novos desafios à comunidade jurídica, tendo em vista que, a depender de seu uso - legítimo ou não - vários são os riscos a que os cidadãos podem ser submetidos, tais como exposição indesejada, discriminação e restrição à liberdade individual.

Diante desses desafios, a proteção dos dados pessoais figura como a disciplina que visa tutelar a privacidade dos cidadãos, sendo o consentimento uma forma de o usuário manter-se informado e autorizar ou não as diversas formas de coleta, processamento e compartilhamento de seus dados pessoais na rede. Visto como um instrumento de autodeterminação informacional e controle para os usuários, o consentimento ocupa um papel central nas várias gerações de leis de proteção de dados pessoais no decorrer do tempo e ao redor do mundo.

Nos diversos regimes jurídicos de proteção de dados, é normal que se tenha uma lei específica regulando a proteção de dados pessoais. Mas no caso brasileiro, essa lei ainda não foi aprovada. Em 2014 foi promulgado o Marco Civil da Internet, que estabelece certos

princípios como a proteção à privacidade e a proteção de dados pessoais. Entretanto, o MCI deixa a cargo de uma lei específica ulterior a regulação detalhada dessa categoria de dados dos usuários.

Existem algumas iniciativas legislativas em andamento que visam regulamentar de maneira ampla a proteção de dados pessoais no Brasil, como o Projeto de Lei do Senado Federal nº 330/2013 – combinado com o 181/2014 e 131/04 – e o Projeto de Lei da Câmara dos Deputados, o 4060/2012.

Contudo, o Projeto de Lei 5.276/2016, de iniciativa do Executivo, foi o que mais recebeu contribuições da sociedade em geral. Com amplo engajamento social por meio de duas consultas públicas, seu anteprojeto recebeu mais de 2.000 contribuições da sociedade civil, comunidade científica, acadêmica e setor empresarial. Por ser aquele que foi construído de maneira mais democrática e colaborativa, bem como por ser hoje visto como o mais maduro na tutela da privacidade dos cidadãos, o Projeto de Lei nº 5.276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, foi o escolhido para a análise deste trabalho.

Ao mesmo tempo, no cenário europeu, um dos mais desenvolvidos na seara de proteção de dados, sendo hoje um dos que mais preza pela proteção à privacidade de seus cidadãos, acaba de ser aprovado o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia, conhecido também como GDPR (*General Data Protection Regulation*). O novo Regulamento revoga a antiga Diretiva 95/46/EC, vigente já desde 1995 na UE, e é hoje uma das legislações mais recentes sobre o assunto, com vigência prevista para maio de 2018.

Diante desse cenário, o presente trabalho analisará o papel do consentimento na proteção de dados pessoais, visando a comparação de como ele é tratado em uma das principais propostas legislativas brasileiras, o PL 5.276/2016, e no Regulamento Geral de Proteção de Dados (RGPD) europeu.

O estudo divide-se em três partes. Em um primeiro momento, será feita uma contextualização da sociedade em rede, com os desafios e riscos das novas tecnologias como o Big Data e o imperativo da vigilância na atual economia da informação. Depois desse contexto, será estabelecida a disciplina da proteção de dados pessoais como a resposta a esses novos riscos e desafios. Para a delimitação do estudo, serão desenvolvidos alguns conceitos básicos, de forma que assim seja examinado o desenvolvimento histórico da proteção de dados pessoais no decorrer do tempo, desde o início com o direito à privacidade até as várias gerações de leis que versam sobre o assunto.

Em um segundo momento, para a delimitação do estudo, será desenvolvido o conceito do consentimento dentro do contexto da proteção de dados, à luz da autodeterminação informativa e como um instrumento para legitimar o tratamento de dados pessoais. Será abordada sua natureza jurídica, possibilidade de revogação, bem como seus pressupostos de validade, a que se chama de adjetivação do consentimento. Além disso, serão consideradas algumas críticas feitas recentemente ao consentimento, bem como as dificuldades e novos desafios desse mecanismo no cenário de constantes evoluções tecnológicas para a tutela de dados pessoais.

Por fim, no terceiro capítulo, será feita uma análise de como o Regulamento Geral de Proteção de Dados traz o consentimento ao longo de seus dispositivos, bem como uma análise de como o PL 5276/16 aborda essa mesma temática, seguindo alguns critérios específicos. Essas duas etapas servirão de base para a comparação do consentimento e seu papel na proteção de dados em ambos os documentos.

Desse modo, este trabalho objetiva contribuir, de forma singela, para o debate jurídico em torno do papel do consentimento na proteção de dados pessoais, além de apresentar uma análise comparada de como ele tem sido abordado por duas disposições normativas tão recentes como o Projeto de Lei 5.276/16 no Brasil e o Regulamento Geral de Proteção de Dados na União Europeia, sem pretensões de esgotar o tema ou ofertar respostas definitivas para todas as questões polêmicas.

CAPÍTULO 1: PROTEÇÃO DE DADOS PESSOAIS NA REDE

1.1 SOCIEDADE EM REDE E ECONOMIA DA INFORMAÇÃO

As revoluções das tecnologias da informação e comunicação nas últimas décadas foram responsáveis por alterar a sociedade a ponto de hoje ela ser reconhecida como "sociedade da informação", "sociedade do conhecimento" ou "sociedade em rede".

Não que conhecimento e informação nunca tenham sido centrais em nossa sociedade[1]. Eles sempre o foram, em todas as sociedades historicamente conhecidas, sendo centrais ao desenvolvimento humano[2].

Mas nas últimas décadas, uma série de adaptações econômicas, sociais e culturais transformaram radicalmente a forma como nós, enquanto indivíduos autônomos, cidadãos e membros de grupos sociais, lidamos com esse novo ambiente informacional. Essa série de mudanças nas tecnologias, organizações econômicas e práticas sociais criaram novas oportunidades na forma como produzimos e trocamos informação, conhecimento e cultura[3].

Dentre as transformações que ensejaram esse novo ambiente nas mais avançadas economias, duas podem ser destacadas. A primeira foi a migração para uma economia centrada na informação, como pode ser visto com a ascensão de serviços financeiros, *software* e ciência; na produção cultural, como na indústria de filmes e música; e na manipulação de símbolos, com a atribuição de valor aos produtos por meio de marcas. A segunda transformação foi a migração para um ambiente de comunicação descentralizado construído com base em processadores de baixo custo e alta capacidade, interconectados em uma rede ubíqua, fenômeno hoje associado à Internet. Essas alterações permitiram, de acordo com Benkler, a emergência de uma "economia da informação em rede" [4].

---

[1] "Frequentemente, a sociedade emergente tem sido caracterizada como sociedade de informação ou sociedade do conhecimento. Eu não concordo com esta terminologia. Não porque conhecimento e informação não sejam centrais na nossa sociedade. Mas porque eles sempre o foram, em todas as sociedades historicamente conhecidas. O que é novo é o facto de serem de base microelectrónica, através de redes tecnológicas que fornecem novas capacidades a uma velha forma de organização social: as redes". CASTELLS, M. A Sociedade em Rede: do Conhecimento à Política. In: CASTELLS, M.; CARDOSO, G. A Sociedade em Rede: Do Conhecimento à Ação Política. Belém: Imprensa Nacional –Casa da Moeda, 2005, p. 17. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/a_sociedade_em_rede_do_conhecimento_a_acao_politica.pdf>. Acesso em setembro de 2017.

[2] BENKLER, Yochai. The wealth of networks: how social production transforms markets and freedom. In: New Haven and London: Yale University Press, 2006, p. 13. Disponível em: <http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf>. Acesso em setembro de 2017.

[3] Ibidem, p. 14.

[4] Ibidem, p. 15.

Paralelo à essa terminologia econômica, está o conceito de "sociedade em rede" elaborado pelo sociólogo Castells:

> A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes[5].

Segundo o autor, as transformações das últimas décadas forneceram novas capacidades a uma velha forma de organização social: as redes, consideradas a "nova coluna vertebral da sociedade"[6]. Hoje, possibilitadas por essa infraestrutura de comunicação e informação, as redes percorrem todos os aspectos da vida, "estando incrustadas no cotidiano do indivíduo e da sociedade"[7].

Essa nova realidade levou inclusive à criação do conceito de onipresença ou ubiquidade dos meios informáticos (*ubiquitous computing*), tal qual já apontava Benkley[8], sendo o uso de smartphones, *wearables*, web 2.0, redes sociais, *cloud computing* e internet das coisas (IoT) exemplos que representam esse fenômeno.

E tal qual aponta Castells, as redes "geram, processam e distribuem informação"[9] a partir do conhecimento acumulado em seus nós. Essa nova configuração da sociedade em rede é marcada pelo nascimento de um novo e verdadeiro "recurso de base" [10]: a acumulação e circulação de dados e informações. Estamos em uma era na qual os dados possuem valor econômico, o que Castells chama de "economia informacional"[11].

Se antes a economia era baseada em um modelo de produção em massa, com fornecimento de grandes quantidades de bens padronizados a baixo custo, hoje a economia

---

[5]CASTELLS, M. A Sociedade em Rede: do Conhecimento à Política. In: CASTELLS, M.; CARDOSO, G. A Sociedade em Rede: Do Conhecimento à Acção Política. Belém: Imprensa Nacional - Casa da Moeda, 2005. p. 20. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/a_sociedade_em_rede_-_do_conhecimento_a_acao_politica.pdf>. Acesso em setembro de 2017.

[6] Ibidem, p. 20.

[7] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 21.

[8] Benkler usa o termo "*pervasive network*". Vide nota de rodapé 4.

[9] CASTELLS, M. Op cit, p. 20.

[10] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 35.

[11] RAMIRO, Livia F. M., DE LUCCA, Newton. A tutela da privacidade e a proteção à identidade pessoal no espaço virtual.In: Direito, Governança e novas tecnologias – V Encontro Internacional do Conpedi Mentevidéu – Uruguai. Coordenadores: Marcelo Eduardo Buza Reilly, Roseane Leal da Silva. Florianópilis: CONPEDI, 2016. Disponível em:< https://www.conpedi.org.br/publicacoes/9105o6b2/v4u5j0t6/lZL7VI9LojzjW2o3.pdf> Acesso em outubro de 2017.

baseia-se em um modelo flexível, com produção customizada e marketing individualizado[12]. E nesse novo cenário, a informação é o novo insumo dessa produção, como preconizado por Benkley[13]. A coleta massiva de informações sobre os usuários, bem como seus hábitos e comportamento, possibilita a oferta de produtos especializados, singularizados e altamente qualificados, em função do mercado e do consumidor[14].

Assim, se as informações sobre os usuários oferecem tantas possibilidades nesse novo modelo de economia, um dos principais insumos de produção é o dado pessoal, aquele que revela aspectos que dizem respeito ao usuário, aquele que "faz referência a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável"[15].

Hoje os dados têm sido caracterizados como "o combustível da economia do século XXI ou o novo petróleo"[16]. Ainda assim, em se tratando de dados pessoais, há uma distinção central entre esses dois insumos de produção: os dados pessoais não são apenas um recurso disponível como o petróleo, mas pelo contrário, são gerados diariamente e em larga escala pelas atividades dos usuários na rede.

Nessa "*data-driven society*", como elabora Steve Lohr[17], cada indivíduo passa a ser considerado um grande centro de produção constante de riquezas, e seus dados representam uma valiosa *commodity*[18] para os negócios na rede, que monetizam grandes quantidades de informações pessoais sobre seus usuários.

---

[12] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.84-90.

[13] BENKLER, Yochai. The wealth of networks: how social production transforms markets and freedom. In: New Haven and London: Yale University Press, 2006, p. 13. Disponível em: <http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf>. Acesso em setembro de 2017.

[14] MENDES, Laura Schertel. Op cit, p. 85-90.

[15] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 157.

[16] TOONDERS, Joris. Data is the new oil of the digital economy. Disponível em: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/. Acesso em: agosto de 2017.

[17] LOHR, Steve. The Promise and Peril of the 'Data-Driven Society'. Disponível em: <https://bits.blogs.nytimes.com/2013/02/25/the-promise-and-peril-of-the-data-driven-society/?_r=0>. Acesso em agosto de 2017.

[18] SOMBRA, Thiago L. Os rumos da agenda de proteção de dados e da privacidade na internet. Disponível em: https://jota.info/artigos/os-rumos-da-agenda-de-protecao-de-dados-e-da-privacidade-na-internet-09072016>. Acesso em julho de 2017.

1.2. BIG DATA E O IMPERATIVO DA VIGILÂNCIA

Tamanha tem sido a geração e circulação de dados nas últimas décadas que o termo mais utilizado nesse sentido é "Big Data". Embora seja uma expressão bastante ampla, vaga e imprecisa[19], algumas definições servem como norte[20].

Doug Laney[21] em 2001 havia definido Big Data com base nos "3V's" volume, variedade e velocidade: uma grande quantidade de dados, de uma grande multiplicidade de fontes e tipos, captados e transmitidos em alta velocidade.

Segundo o Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS, Big Data é o "conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores" [22].

Já o Article 29 Working Party[23] relaciona Big Data ao crescimento exponencial tanto na disponibilidade quanto no uso automatizado de informação. Assim, não se trata apenas de um grande volume de dados. São conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grande porte, que são amplamente analisados usando algoritmos de computador[24]. Assim, Big Data diz respeito à capacidade de procurar, analisar, agregar e cruzar todos esses dados com o intuito de extrair resultados e benefícios[25].

---

[19] *"Big data is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics."* Kate Crawford and Jason Schultz. Big data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. In: Boston College Law Review, vol. 55, 2014. Disponível em: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>. Acesso em outubro de 2017.

[20] GOMES, Rodrigo Dias de Pinho. Desafios à privacidade: Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf>. Acesso em setembro de 2017.

[21] ENISA. Privacy by Design in Big Data.P. 10. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: outubro de 2017. Hoje o conceito já foi estendido para 4Vs (veracidade), 5Vs (variabilidade), 6Vs (valor) e até 7Vs (visualização).

[22] Big data no projeto Sul Global. Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big_-Data_PT-BR_v2.pdf>. Acesso em: outubro de 2017.

[23] O Article 29 Working Party é uma organização de caráter consultivo e independente, criada pela Diretiva 95/46/EC do Parlamento Europeu, composta por representantes de todas as Autoridades de Proteção de dados da União Europeia. Tradução livre da definição disponível em: < http://ec.europa.eu/justice/data-protection/>. Acesso em outubro de 2017.

[24] Conceito extraído do documento "Opinion 03/2013 on purpose limitation" elaborado pelo Article 29 Working, Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em outubro de 2017.

[25] BOYD, Danah. CRAWFORD, Kate. Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society . Vol. 15, Issue 5.

O termo "análise de big data"[26] refere-se justamente a todo esse processo de coletar, organizar e combinar dados para inferências, descobertas de padrões e previsões comportamentais.

Um dos resultados da análise de Big Data é inclusive a criação de novas informações com base no conjunto de dados já coletados. Como o próprio nome diz, a "utilização secundária dos dados" consiste na utilização de dados com finalidade diversa daquela da coleta inicial, e por meio da combinação ou cruzamento de dados, informações derivadas são produzidas e acabam adquirindo um novo valor. Dessa forma, o valor das informações obtidas não reside apenas na capacidade de armazenamento de um grande volume de dados, mas principalmente na possibilidade de obtenção de novas informações a respeito dos usuários a partir do tratamento desses dados[27].

Exemplo disso é o que pode ocorrer com dados pessoais voltados à área da saúde[28]. Alguns aplicativos de celular coletam dados pessoais dos usuários como batimentos cardíacos, quantidade de passos e hábitos de dieta. O objetivo inicial é o de prover aos usuários informações sobre sua condição cardíaca e sua saúde em geral. No entanto, se cruzados, esses dados podem ser valiosos para empresas de seguro determinarem valores de planos de saúde, por exemplo, ou para profissionais de saúde investirem em públicos-alvo específicos.

No modelo de negócios da vigilância, as empresas oferecem serviços "gratuitamente", quando na verdade os usuários pagam em forma de dados pessoais. E essas empresas conseguem manter-se vendendo esses dados a outras empresas que se interessam, visto que conseguem extrair deles um novo valor. Não é por acaso que se fala nos chamados "corretores de dados" ou indústria dos *data brokers*, que movimenta cerca de 156 bilhões de dólares por ano[29]. Empresas como Acxiom e Experian[30] têm como nicho a compra e venda de grandes bancos de dados pessoais para propósitos como prevenção de fraudes, análise de

2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878 >, p. 663. Acesso em: outubro de 2017.

[26] Privacy by Design in Big Data. ENISA. P. 12. Disponível em: <https://www.enisa.europa.eu/publications/big-data-protection>. Acesso em: outubro de 2017.

[27] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 33.

[28] Exemplo citado no Privacy by Design in Big Data. ENISA. P. 13. Disponível em: <https://www.enisa.europa.eu/publications/big- data-protection>. Acesso em: outubro de 2017.

[29]PASQUALE, Frank. The Dark Market for Personal Data. Disponível em: <https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html> Acesso em outubro de 2017.

[30]RIGHTS, Coding. Notícia "Estudo de Princeton expõe vigilância descontrolada dos trackers na Web". Disponível em: < https://antivigilancia.org/pt/2016/06/webcensus/> Acesso em agosto de 2017.

crédito e marketing. Elas oferecem produtos para fins de segmentação da população, autenticação de indivíduos e descoberta de tendências comportamentais[31].

Se nesse novo cenário, como já visto, a informação é o grande insumo de produção, a vigilância sobre os usuários – possíveis consumidores- e a captação de seus dados são estratégias adotadas para uma produção flexível e marketing individualizado. O "imperativo de vigilância" [32] seria exatamente a habilidade de monitorar os comportamentos e hábitos dos consumidores para diferenciar e alcançar nichos específicos de mercado. Seria a estratégia utilizada para um marketing efetivo, com a customização de serviços e produtos.

Nunca houve dúvida de que o Estado já possuía meios para exercer vigilância e habilidade para monitorar, interceptar e captar dados visando, em tese, a segurança nacional e o bem-estar social. Foi cunhado nesse sentido, inclusive, o termo "vigilância digital" (*digital surveillance*). Os escândalos, contudo, sobre espionagem na internet e meios de comunicação que atingiram a Agência Nacional de Segurança dos EUA (NSA) em 2013 deixaram claro que o Estado estava a violar a integridade, o sigilo e a confidencialidade do fluxo de informações dos cidadãos. As revelações de Edward Snowden[33] revelaram de forma inédita os riscos a que os cidadãos estão submetidos quanto à esfera estatal.

Mas se antes a discussão sobre vigilância digital e os danos causados pelo processamento e fluxo de dados na sociedade restringia-se à ameaça do enorme poder do Estado[34], como que na figura do "Big Brother" de George Orwell, hoje a discussão abrange também o setor privado, que utiliza massivamente dados pessoais para atingir seus objetivos econômicos. Como afirma Laura Schertel[35], a ameaça passa a ser representada pelos "pequenos irmãos", milhares de empresas que constantemente coletam, armazenam e processam dados dos usuários, consumidores finais ou não.

Assim, se antes o termo "vigilância" era utilizado para se referir a fenômenos específicos de controle, relacionados a investigações policiais e inteligência governamentais,

---

[31]TEIXEIRA, Lucas. Data Brokers e Profiling: vigilância como modelo de negócios. Disponível em: < https://antivigilancia.org/pt/2015/05/data-brokers-e-profiling-vigilancia-como-modelo-de-negocios/> . Acesso em outubro de 2017.

[32]MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.91.

[33]Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded Acesso em outubro de 2017.

[34]GONÇALVES, Andrey F. L., BERTOTTI, Monique e MUNIZ, Veyzon C. O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais. In: Doutrinas Essenciais do Direito Constitucional. Revista dos Tribunais online. Vol. 08/2015, p. 597-614.

[35]MENDES, Laura Schertel. Op. cit., p.83.

hoje a vigilância digital tornou-se uma característica do cotidiano na sociedade contemporânea, invadindo cada momento da vida e se apresentando como um traço próprio das relações de mercado[36]. Os mais diversos tipos de entidades realizam diariamente a vigilância dos cidadãos, consumidores e empregados, que têm seus dados pessoais coletados, processados e tratados diuturnamente[37].

Tal vigilância não está distante da realidade brasileira. De acordo com o Relatório "Big Data no projeto Sul Global" produzido pelo Instituto de Tecnologia & Sociedade do Rio de Janeiro em 2016[38], embora o uso de Big Data no Brasil seja relativamente recente, grandes volumes de dados estão sendo gerados pelos cidadãos brasileiros com o uso cada vez maior de aplicativos, websites e *software* para manter seus registros em *cloud computing*, diversos conjuntos de dados estão sendo publicados online por projetos de transparência do Governo, e *startups* e até empresas bem estabelecidas estão à procura de novos dados para promover novos aplicativos ou manipular informações a fim de patrocinar produtos lucrativos.

Nesse cenário, as técnicas do atual modelo de negócios em rede trazem consigo novos desafios à comunidade jurídica, tendo em vista que, a depender de seu uso – legítimo ou não -, vários são os riscos a que os indivíduos podem ser submetidos dentro do imperativo da vigilância. A combinação dos mecanismos automatizados de tratamento de dados permite a obtenção de informações pessoais sobre os cidadãos que, por sua vez, não conseguem determinar quais delas estão sendo utilizadas para a tomada de decisões que influenciem na sua vida, quer seja pelo governo, quer seja por empresas privadas.

Tais decisões, quer econômicas, políticas ou sociais, são muitas vezes fundamentadas com base na construção e classificação de perfis virtuais dos usuários, perfis que por muitas vezes não chegam a representar de fato a personalidade dos indivíduos[39]. Visto que estamos deixando cada vez mais rastros de nossa vida diária, cada vez mais "pegadas digitais", a depender do uso dessas técnicas, grandes são os perigos de exposição indesejada, discriminação e restrição à liberdade individual.

---

[36] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 113.

[37]MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.22.

[38]Relatório disponível em: https://itsrio.org/wp-content/uploads/2017/01/ITS_Relatorio_Big-Data_PT-BR_v2.pdf Acesso em agosto de 2017.

[39]MENDES, Laura Schertel. Op. cit., p. 22.

Na "sociedade da vigilância", como define Rodotà[40], a contrapartida necessária para se obter um bem ou serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. E nessa troca, não é apenas o patrimônio da pessoa que está envolvido, e sim o seu próprio eu, a exposição de sua própria *persona*, colocando em risco sua privacidade. Para o autor, as consequências dessa exposição vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito.

A visão de Rodotà levanta um importante questionamento acerca dos dados pessoais abordados até o momento. Foi colocado que hoje em dia os dados pessoais são considerados recursos de base e objetos de grande valor para comercialização na economia da informação. Mas ao mesmo tempo, acabam por formar um perfil virtual dos usuários na sociedade em rede, relacionando-se à própria personalidade dos usuários.

Diante dos riscos apontados nessa nova "sociedade da vigilância", a proteção de dados pessoais figura como uma forma de proteger o usuário, como se verá adiante. Mas antes, é preciso responder a um questionamento: afinal, qual a natureza do bem a ser tutelado quando se fala em proteção de dados pessoais? Porque se considerados apenas por seu grande valor econômico e capacidade de comercialização, uma abordagem possível seria a da proteção a um direito de propriedade. Mas se considerados pela formação de uma representação pessoal de uma pessoa, talvez a abordagem mais adequada seria a da proteção a um direito de personalidade.

A resposta para essa questão depende, primeiro, do estabelecimento de alguns conceitos e definições, que mais à frente ajudarão a definir uma concepção adequada para um regime de proteção de dados pessoais.

1.3. INFORMAÇÕES, DADOS PESSOAIS E FORMAS DE TRATAMENTO

Como foi visto até o momento, "dados" e "informações" podem ser considerados pontos de referência nessa nova sociedade em rede e economia da informação. Em várias circunstâncias, os dois vocábulos se sobrepõem. Ambos servem para representar um fato, um

[40]Rodotà defende inclusive a transformação da "sociedade da informação" na "sociedade da vigilância", exatamente pela ideia de que a vigilância invade cada momento da vida. RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 113.

determinado aspecto de uma realidade. Contudo, cada um carrega um peso particular a ser levado em conta.

Segundo Danilo Doneda, o "dado" apresenta uma conotação um pouco mais primitiva e fragmentada[41], como uma espécie de pré-informação ou uma informação em potencial. O dado pode se transformar em informação caso seja comunicado, recebido e compreendido. Já a informação faz referência a algo além da representação contida no dado. Ela já pressupõe uma fase inicial de depuração do conteúdo do dado e pode apresentar-se em diversas formas, como a gráfica, fotográfica e acústica.

Dentro do conceito de "informação" está a "informação pessoal"[42], aquela que possui um vínculo objetivo com uma pessoa, revelando algo sobre ela. Esse vínculo significa que a informação se refere às características ou ações de determinada pessoa, como o nome civil ou domicílio, bem como dados referentes ao seu consumo e opiniões que manifesta. Esse vínculo, segundo Doneda, é o que afasta outras categorias de informações que, embora façam referência a uma pessoa, não são propriamente informações pessoais, como as opiniões alheias sobre uma determinada pessoa ou mesmo sua produção intelectual. O que identifica uma informação pessoal é quando o objeto da informação é a própria pessoa. Assim, o mecanismo pelo qual se pode caracterizar uma determinada informação pessoal é justamente, como demonstra o autor, "o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta"[43].

Por tais motivos, essas informações pessoais merecem tutela jurídica, uma vez que, por terem como objeto a própria pessoa, constituem um atributo de sua personalidade[44]. Mas essa tutela "visa à proteção da pessoa e de sua personalidade, e não dos dados *per se*"[45], o que começa a delinear a resposta ao questionamento da seção anterior a respeito da natureza do bem a ser tutelado com o regime de proteção de dados pessoais.

---

[41]DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 152.

[42]Pierre Catala, ao traçar um esboço de uma teoria jurídica da informação, classificou-a em quatro modalidades: (i) as informações relativas às pessoas e seus patrimônios; (ii)as opiniões subjetivas das pessoas; (iii) as obras do espírito; (iv) as informações que descrevem fenômenos, coisas e eventos. CATALA, Pierre. "Ebauche d'une théorie juridique de l'information", in: Informatica e Diritto, ano IX, jan-apr. 1983, p. 22 APUD DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 152

[43] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 157.

[44] CATALA, Pierre. Apud DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 157.

[45] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 56.

Com relação ao conceito de dados pessoais, pode-se dizer que são "os fatos, comunicações e ações que se referem a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável"[46]. De acordo com a consideração nº 26 do Regulamento (EU) 2016/79[47], dado pessoal seria "qualquer informação relativa a uma pessoa singular identificada ou identificável", sendo que "para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular"[48].

Seguindo a lógica dessa definição, dados anônimos seriam aqueles fora da tutela jurídica da proteção de dados exatamente por não serem relacionados "à pessoa identificada ou identificável"; aqueles que fazem referência a pessoas indeterminadas e podem ser utilizados para fins estatísticos, como forma de proteger as pessoas que tiveram seus dados coletados e armazenados. Mas este ainda é um ponto que merece cautela, visto que diante da evolução da tecnologia, a anonimização de dados pode ser reversível[49]. Assim, por ser ainda possível a reidentificação, esses fragmentos "aparentemente inócuos de informação pessoal"[50] não podem ser totalmente desconsiderados em uma regulação de proteção de dados.

Prosseguindo sobre o conceito e natureza dos dados pessoais, diante do fato de que hoje em dia eles possuem grande valor e são comercializados em larga escala, é possível encontrar um debate doutrinário acerca de um possível direito de propriedade sobre os dados pessoais[51]. Os defensores dessa concepção proprietária apontam para o fato de que essa

[46] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 56.

[47] Regulamento (UE0) 2016/679 do parlamento europeu e do conselho de 27/04/2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: < http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EM>

[48] A consideração ou "considerando" – como utiliza Laura Schertel - nº 26 continua: "Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a essoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica". Disponível em: < http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EM> Acesso em agosto de 2017.

[49] "Sempre existirá a possibilidade de uma base de dados anonimizada ser agregada a outra para a sua reidentificação. É o que se costuma chamar de entropia da informação (Ohm, 2010: 1749), que é o uso de uma informação auxiliar para a reversão do processo de anonimização" Bioni, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[50] MENDES; S., L.; DONEDA, D. Marco Jurídico Para a Cidadania Digital: Uma Análise Do Projeto De Lei 5.276/2016. Revista de Direito Civil Contemporâneo, v. 9/2016, p. 35–48

[51] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 121.

comercialização acarreta uma grande externalidade negativa, a saber a violação ao direito à privacidade das pessoas que não consentiram na transmissão de seus dados. E como forma de minimizar tais danos, indicam como solução a internalização do custo por quem usa o dado, como forma de pagamento para o seu detentor[52].

Contudo, Laura Schertel alerta para os riscos e problemas de uma concepção proprietária dos dados pessoais, sob a forma de três argumentos principais[53]. Como primeiro argumento, ela aponta para o risco de violação ao princípio da igualdade, uma vez que é possível inferir que apenas parte da população usufruiria do direito à proteção de dados nesse molde. Os beneficiados por esse direito possivelmente seriam apenas aqueles com condições financeiras para optar pela proteção de seus dados pessoais em detrimento da remuneração a ser paga pelo interessado a utilizá-lo.

O segundo argumento diz respeito à supressão da individualidade e o surgimento de indivíduos direcionados ao mercado, ou "*market-oriented*"[54], como ela denomina. As pessoas poderiam moldar suas personalidades para moldar seus dados e assim conseguir melhores condições de comercialização de suas informações pessoais, o que não apenas suprimiria como nivelaria individualidades.

E o terceiro argumento seria a ameaça ao próprio Estado Democrático de Direito. De acordo com esse raciocínio, no momento em que a proteção de dados fosse substituída por um modelo de mercado, nem todos os cidadãos teriam mais a garantia de proteção de sua personalidade e privacidade, o que ameaçaria sua liberdade de comportamento, pensamento e ação. Como o funcionamento de uma sociedade democrática depende exatamente da capacidade autônoma de ação e participação de cada indivíduo para a formação da vontade comum, a própria democracia estaria em risco.

Por tais motivos, tratar o direito à privacidade e aos dados pessoais sob uma concepção de direito de propriedade seria, segundo a autora, abrir a possibilidade para sérios riscos à dignidade humana, à personalidade e ao próprio Estado Democrático de Direito.

De fato, os dados pessoais na economia da informação possuem grande valor e capacidade de comercialização, como aponta a premissa da concepção proprietária dos dados pessoais. Contudo, os mesmos dados, assim como as demais informações extraídas deles,

[52] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 121.
[53] Ibidem, p. 122.
[54] Ibidem, p. 94.

podem constituir uma representação virtual dos indivíduos, que são conhecidos por meio de uma sequência de códigos e números computadorizados, a partir dos quais são tomadas decisões que afetam sua vida e personalidade[55].

É por isso que a natureza do bem protegido, a própria personalidade a que os dados pessoais se referem, exige a compreensão da proteção dos dados pessoais não como um direito à propriedade, mas sim como uma espécie de direito da personalidade. A regulação do direito à proteção de dados pessoais, portanto, não é da relação entre proprietários e seus bens, de ordem de propriedade, e sim de ordem multidimensional[56], envolvendo o equilíbrio dos direitos de proteção, defesa e participação do indivíduo nos processos comunicativos. Dessa forma, o direito à proteção de dados pessoais deve ser admitido não como uma garantia de propriedade, mas como uma "proteção da personalidade do indivíduo contra os riscos ocasionados pela coleta, processamento e circulação dos dados pessoais"[57].

No mesmo raciocínio, Danilo Doneda defende uma tutela dinâmica dos dados pessoais, que acompanhe sua circulação, sem concentrar-se no sujeito, mas que ainda os considere como uma extensão de sua personalidade:

> A informação pessoal em um certo sentido pode ser desvinculada da pessoa e tornar-se exterior a esta: ela pode circular, submeter-se a um certo tratamento, ser comunicada, etc. Porém, até o ponto em que continue sendo uma informação "pessoal", isto é, que continue a identificar a pessoa a qual se refere, ela mantém com esta um vínculo específico, e sua valoração deve partir deste dado básico. Por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual se refere – como representação direta da personalidade - tal informação deve ser entendida como uma extensão da sua personalidade.[58]

Ainda, quando se fala na proteção de dados pessoais, muito se faz referência à expressão "tratamento de dados pessoais", que designa o conjunto de técnicas a que os dados pessoais podem ser submetidos, com o objetivo de refinar as informações e torná-las valiosas ou úteis. Ele é um processo complexo que envolve diversos mecanismos, mas que pode ser dividido para fins didáticos em três momentos: a coleta, o processamento e a difusão dos dados[59], que serão explicados brevemente a seguir.

A coleta pode ser considerada a primeira fase do tratamento de dados. A empresa ou o controlador de dados obtém as informações pessoais do usuário. Nem sempre essa obtenção ocorre de forma secreta, sem que o cidadão tenha conhecimento da coleta. Como

[55] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.123-124.
[56] Ibidem, p. 124.
[57] Ibidem, p. 124.
[58] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 168.
[59] MENDES, Laura Schertel. Op. cit., p.94.

afirma Laura Schertel, muitas vezes ocorre o contrário: o usuário participa ativamente no processo de concessão de suas informações, mesmo que muitas vezes sem consciência das consequências disso. Isso pode ocorrer com o uso de smartphones, *wearaebles*, cartões de créditos, entre outros. As principais fontes de dados dos cidadãos são transações comerciais, censos e registros públicos, pesquisas de mercado e estilo de vida, sorteios e concursos, comercialização e cessão de dados, tecnologias de controle na internet[60].

Já o processamento pode ser considerado a segunda fase do tratamento, quando os dados pessoais são submetidos a várias técnicas para lapidá-los e transformá-los em informações úteis para as empresas, por exemplo. É nesse momento que ocorre a classificação dos usuários e sua segmentação em grupos diversos. Em se tratando da relação de consumo, por exemplo, é aqui o momento em que a empresa atribui valores diferentes para seus clientes, analisa as opções de demanda e conhece os diferentes segmentos para direcionar sua publicidade. Técnicas como mineração de dados (*data mining)*, construção de perfil (*profiling*) e sistema de avaliação (*scoring*) são utilizadas nessa fase de tratamento.

De forma simplificada, a técnica do *data mining* tem o objetivo de extrair padrões a ponto gerar regras e permitir a classificação de pessoas ou objetos. Já o *profiling* possibilita a construção de perfis, ou seja, a reunião de inúmeros dados sobre uma pessoa que expressam uma completa e abrangente imagem sobre a sua personalidade. O objetivo dessa técnica é a obtenção de uma imagem detalhada e confiável, visando à previsibilidade de padrões de comportamento, gostos, hábitos de consumo e preferência do usuário[61]. E o *scoring* é a técnica que objetiva identificar os usuários que têm maior valor para a empresa, para que eles sejam alvos de promoções e estratégias de fidelização de clientes. Além disso, ela permite dimensionar os riscos de contratação de possíveis futuros clientes, indicando quais consumidores apresentam um menor risco de inadimplência[62].

Por fim, a difusão ou cessão de dados pode ser considerada o terceiro momento do tratamento de dados. Como já foi mencionado ao se falar do "mercado de negócios da vigilância", hoje há uma "indústria de bancos de dados"[63] cuja finalidade é propiciar aos setores interessados, por meio da comercialização ou cessão, dados sobre categorias de usuários. A

[60] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.96.
[61] Ibidem, p.111.
[62] Ibidem, p.112.
[63] SOLOVE, Daniel. The digital person: technology and privacy in the information age. New York: New York University, 2004, p. 19. Apud. MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.117.

difusão pode ocorrer ainda com o compartilhamento de bancos de dados, prática comum, por exemplo, entre empresas de um mesmo grupo empresarial.

Percebe-se que a evolução das técnicas no tratamento de dados pessoais possibilitou a combinação de dados em seu estado bruto, a princípio sem muita importância, para a criação de novas informações úteis e valiosas. Contudo, ao passo que essas técnicas ampliaram as oportunidades de ação dos indivíduos, elas também ampliaram os riscos a que os indivíduos podem ser submetidos.

Afinal, em se tratando da fase da coleta, por exemplo, é de se imaginar o recolhimento de dados sem que o usuário tenha consentido ou ao menos tenha sido comunicado. Além disso, pode não haver o respeito à finalidade para o qual a coleta foi realizada. Em se tratando da fase de lapidação da informação, a fim de se buscar informações mais completas sobre os hábitos e comportamentos dos usuários, as técnicas como *data mining*, *profiling* e *scoring* podem levar à criação de perfis ou padrões que não correspondem à realidade ou discriminem seus usuários. Sem contar com a ampliação desses riscos com a possibilidade de cessão, transferência, compartilhamento e comercialização de dados pessoais.

Embora esse repasse a terceiros citado por último seja complexo e polêmico, é certo que, por mais que o desenvolvimento dos setores empresariais dependa da informação como um insumo de produção na *data-driven society*, deve haver também um equilíbrio entre essa livre-iniciativa e a proteção adequada à privacidade, liberdade e igualdade dos cidadãos.

Diante desse cenário complexo, o direito à proteção de dados pessoais surge como um novo direito à privacidade, atrelado a um direito de personalidade, consubstanciado na proteção e controle das próprias informações pessoais por parte dos usuários, como se verá adiante.

1.4. DA PRIVACIDADE À PROTEÇÃO DOS DADOS PESSOAIS: DO SIGILO AO CONTROLE[64]

A origem do termo "proteção de dados pessoais" tem como cerne o desenvolvimento do próprio conceito de privacidade. O início dos debates doutrinários a respeito do direito à privacidade ocorreu em decorrência da utilização de novas tecnologias que

[64] O título da seção faz referência à obra do professor Danilo Doneda "Da privacidade à proteção de dados pessoais" e ao termo utilizado por Rodotà, ao discorrer sobre o caminho da privacidade do indivíduo até a coletividade "do sigilo ao controle". RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 23-40.

permitiram de forma inédita o acesso e a divulgação de fatos relativos à esfera privada dos indivíduos.

Um artigo pioneiro sobre a privacidade foi o elaborado por Warren e Brandeis, intitulado "*The right to privacy*", em que os autores denunciavam como os jornais, com seus novos aparatos tecnológicos, estavam a invadir o domínio da vida privada[65]. Nesse artigo, o direito à privacidade foi, de maneira inédita, relacionado à inviolabilidade da personalidade, de forma a romper com a antiga tradição de proteção à privacidade como forma de propriedade.

Nessa época, surge o direito a ser deixado só (*right to be let alone*), com um viés individualista e negativo[66], associado ao isolamento e reclusão[67], no sentido de exigir absoluta abstenção do Estado na esfera privada individual como forma de garantia da privacidade dos cidadãos. A forma de tutelar a privacidade das pessoas era por meio do segredo, do sigilo, de forma a se evitar a circulação de informações relacionadas à personalidade, à vida privada dos indivíduos.

Contudo, como foi visto, a evolução das tecnologias nas últimas décadas e o crescente protagonismo da informação na sociedade criaram um cenário de intensa circulação de dados pessoais. E nesse novo ambiente, a tutela individualista de se apenas evitar intromissões exteriores[68] já não era mais suficiente para proteger a privacidade dos cidadãos. Nesse sentido, aponta Stefano Rodotà:

> (...) não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e fortalece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem[69].

---

[65] "*To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.*" WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy, In: *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), p. 196. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf >. Acesso em agosto de 2017.

[66] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.29.

[67] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 1.

[68] Ibidem, p. 24.

[69] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p.13.

Da discussão acerca da violação do direito de celebridades fotografadas em situações embaraçosas ou íntimas, como no artigo de Warren e Brandeis, o debate sobre o direito à privacidade voltou-se para o risco à personalidade de milhares de cidadãos cujos dados pessoais são coletados, processados e transferidos por organismos estatais e privados, a partir de modernas tecnologias da informação, tomando uma dimensão coletiva e relacionada ao controle.

Nesse novo cenário, era necessário que os indivíduos tivessem controle sobre as informações que lhe diziam respeito e que certamente estariam circulando pela rede:

> Essa evolução gera novos e significativos contextos. As informações fornecidas pelas pessoas para que obtenham determinados serviços são tais, em quantidade e qualidade, que possibilitam uma série de usos secundários, especialmente lucrativos para os gestores dos sistemas interativos. Estes, elaborando as informações obtidas quando do fornecimento dos serviços, podem "criar" informações novas (perfil de consumo individual ou familiar, análises de preferência, informações estatísticas, etc.) que interessam a outros sujeitos, a quem estas informações podem ser vendidas.
>
> E não se pode dizer que tal comportamento esteja em contradição com a tendência, anteriormente referida, segundo a qual existem categorias inteiras de informações pessoais (como aquelas de conteúdo econômico) cuja divulgação é oportuna ou necessária: publicidade e controle não são termos contraditórios, como são publicidade e sigilo. Exatamente onde se admitir a máxima circulação de informações de conteúdo econômico, deve-se permitir aos interessados exercitar um real poder de controle sobre a exatidão de tais informações, sobre os sujeitos que as operam e sobre as modalidades de sua utilização[70].

Assim, o autor demonstra o surgimento de um caminho para a proteção da privacidade na economia da informação em rede, não mais ligada ao sigilo como era antes, mas sim ao controle. Segundo ele, privacidade e controle não são termos contraditórios, mas sim termos que, se combinados, permitem uma real proteção ao indivíduo inserido nesse contexto em que os dados pessoais têm valor econômico. De um direito com uma dimensão negativa, o direito à privacidade passa a ser considerado uma garantia de controle do indivíduo sobre suas próprias informações.

O objeto do direito à privacidade é dessa forma ampliado. A noção técnica da esfera privada é enriquecida e passa a ser o número crescente de situações juridicamente relevantes, com o potencial de comunicação de dados que podem ser traduzidos em informações. Privado deixa de significar necessariamente "secreto" e passa significar "pessoal"[71]. Assim, o titular do

[70] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p.46.
[71] Ibidem, p. 93.

direito à privacidade pode exigir formas de circulação controlada, e não apenas interromper o fluxo das informações que lhe digam respeito.

O perfil de privacidade foi, assim, reinventado[72], de forma que aos poucos deixou de se estruturar em torno do eixo "pessoa-informação-segredo" (paradigma chamado "*zero relationship*"), para se estruturar em torno do eixo "pessoa-informação-circulação-controle"[73]. E com essa mudança de eixo, o direito à privacidade transformou-se para fazer emergir a dimensão da proteção de dados pessoais, à medida em que surgiram novas formas de tratamento informatizado de dados.

Dessa maneira, a proteção da privacidade na sociedade da informação na forma da proteção de dados pessoais foi um modo de proporcionar não apenas a tranquilidade e o isolamento dos indivíduos, mas meios para construir e consolidar uma esfera privada própria[74], agora dentro de um contexto de intensa circulação de dados.

A proteção de dados pessoais surge, então, como uma possibilidade de tutelar a personalidade do indivíduo contra os potenciais riscos a serem causados pelas técnicas de tratamento de dados pessoais[75], como as mencionadas na seção anterior. E a sua função não é a de proteger os dados *per se*, mas sim a pessoa que é titular desses dados.

Uma vez que as informações pessoais são intermediárias entre a pessoa e a sociedade, permitindo a criação de verdadeiros perfis, a personalidade de um indivíduo pode ser violada com a divulgação inadequada e utilização de informações armazenadas a seu respeito[76]. E por constituírem a personalidade da pessoa, os dados pessoais merecem tutela jurídica, para assegurar sua liberdade e igualdade.

Assim, não há uma dicotomia entre privacidade e tecnologia, da mesma forma como não há entre privacidade e controle, como apontado anteriormente por Rodotà. O desenvolvimento da tecnologia deve ser harmonizado com a privacidade dos cidadãos, da mesma forma que deve ser rejeitada a ideia de que a tecnologia é responsável pela perda da privacidade na sociedade contemporânea[77].

---

[72] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p.15.
[73] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 23.
[74] Ibidem, p. 25.
[75] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.32.
[76] DONEDA, Danilo. Op. cit., p. 27.
[77] MENDES, Laura Schertel. Op. cit., p.35.

Nesse raciocínio, o direito à privacidade transforma-se para dar origem à proteção de dados pessoais de modo a se adaptar aos desafios impostos pela técnica. De acordo com Danilo Doneda, a disciplina dos dados pessoais "manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias"[78]. Segundo Laura Schertel, a proteção de dados pessoais pode ser compreendida como uma "dimensão do direito à privacidade, que, por consequência, partilha dos mesmos fundamentos: a tutela da personalidade e da dignidade do indivíduo"[79].

A proteção de dados pessoais passa a ser marcada, além do seu caráter coletivo, pelo controle sobre as próprias informações, pela possibilidade de um sujeito conhecer, controlar, endereçar e interromper o fluxo das informações a ele relacionada[80], o que se chama também de autodeterminação informativa.

Na evolução do conceito de privacidade até a chegada da proteção de dados pessoais, a decisão do Tribunal Constitucional Alemão de 1982, do julgamento da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" é considerada uma referência. Nesse julgamento histórico, o Tribunal levou às últimas consequências o conceito do livre controle do indivíduo sobre o fluxo de informações da sociedade e decidiu pela inconstitucionalidade parcial da Lei de Recenseamento, argumentando sobre a existência de um direito à autodeterminação informativa[81].

Essa Lei de Recenseamento visava coletar dados dos cidadãos sobre suas profissões, moradias e locais de trabalho para fornecer à administração pública informações sobre crescimento e distribuição da população pelo país. Aqueles que se recusassem a responder estariam sujeitos à multa. E para averiguar a veracidade das informações coletadas, havia a previsão de comparação com os registros públicos. Ademais, havia a possibilidade de transmissão desses dados para órgãos públicos federais, conquanto anonimizados. Frente à essa lei, várias reclamações foram ajuizadas com base na violação direta ao art. 21 da Constituição alemã, que protege o livre desenvolvimento da personalidade[82].

O Tribunal conheceu da reclamação e, no mérito, confirmou a constitucionalidade da lei, declarando nulos os dispositivos sobre a comparação e transferência de dados. Mas o

[78] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 204.
[79] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.35.
[80] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 96.
[81] MENDES, Laura Schertel. Op. cit. p.30.
[82] Ibidem, p.31.

grande mérito do julgamento foi a criação de um marco para a teoria da proteção de dados pessoais, ao reconhecer um direito subjetivo fundamental – o direito à autodeterminação informativa - e elevar o indivíduo a protagonista no processo de tratamento de seus dados. A Corte afirmou que a Constituição alemã protege o indivíduo contra o tratamento indevido de dados pessoais "por meio do direito fundamental ao livre desenvolvimento da personalidade, segundo o qual o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade"[83].

De forma breve, foi exposta a evolução do conceito de privacidade até se chegar a uma ideia de proteção de dados pessoais; de uma definição original do direito a ser deixado só até o direito de controle sobre as informações e determinação da forma de construção da esfera privada.

Mas não só o conceito de privacidade evoluiu, como a própria disciplina de proteção de dados pessoais, a ponto de se falar em gerações de leis de proteção de dados pessoais. Assim, para a devida compreensão do consentimento como forma de proteção de dados e para a compreensão adequada do contexto em que se situam as duas normativas que serão objeto de análise no presente trabalho, será abordado, de forma rápida, o desenvolvimento geracional das leis de proteção de dados pessoais.

1.5. GERAÇÕES DE LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Da mesma forma que houve uma evolução do conceito de privacidade até se chegar à ideia de proteção de dados pessoais e autodeterminação informativa, é possível notar também um desenvolvimento na disciplina da proteção de dados no decorrer das iniciativas legislativas para a tutela de dados pessoais. Para uma breve exposição desse processo de transformação, será utilizada a análise geracional, inicialmente proposta por Mayer-Schönberger, que oferece uma perspectiva histórico-evolutiva para a compreensão da proteção de dados[84].

A primeira geração de normas de proteção de dados pessoais surgiu na década de 70, como reação ao processamento eletrônico de dados nas Administrações Públicas e Empresas privadas, e à centralização dos bancos de dados em grandes bancos de dados

[83] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.32.
[84] MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The Mit Press, 2001. Apud. MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.32.

nacionais. Exemplos são as leis do Estado alemão de Hesse de 1970, a Lei de Dados da Suécia de 1973, além do *Privacy Act* norte-americano de 1974[85]. Num contexto de Estado Social que requeria, para o funcionamento de sua burocracia e planejamento, a coleta e o processamento de dados dos cidadãos, a ideia era criar um grande e unificado banco de dados.

Nos EUA, o exemplo mais famoso é o caso do National Data Center, projeto de um centro que conteria dados de todos os cidadãos americanos, desde registros de impostos a registros criminais. O projeto nunca chegou a ser construído, tendo em vista que se chegou à conclusão de que os direitos e liberdades fundamentais dos cidadãos americanos estariam sob ameaça pela coleta ilimitada e centralização de dados pessoais por parte do governo americano.

A principal característica dessa geração de leis de proteção de dados pessoais é sua perspectiva funcional de buscar controlar os bancos de dados de forma *ex ante*, condicionando o seu funcionamento à licença prévia ou registro[86].

Contudo, e conforme aponta Laura Schertel, se esses projetos de dados não foram construídos, isso deve-se não às reivindicações sociais, mas sim ao desenvolvimento tecnológico que multiplicou o armazenamento e processamento de dados de forma descentralizada. Essa mudança tecnológica "expôs a fragilidade da regulamentação de normas de primeira geração que estabeleciam procedimentos em detrimento de direitos"[87], surgindo a necessidade de alteração legislativa.

Assim surgiu a segunda geração de proteção de dados pessoais a partir do final da década de 1970, como consequência da "diáspora" dos bancos de dados informatizados e unificados[88]. Exemplos de leis são as da França de 1978 e da Áustria. A característica básica de diferenciação dessa geração de leis é sua estrutura, que não mais gira em torno de procedimentos, e sim da consideração da privacidade em si e proteção dos dados pessoais como uma liberdade negativa. Outra mudança é a ampliação dos poderes das autoridades administrativas encarregadas da proteção de dados[89].

Laura Schertel[90] mais uma vez mostra uma controvérsia suscitada por essa geração de leis: a efetividade do consentimento do cidadão e o real exercício de liberdade de escolha

[85] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 207.
[86] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.39.
[87] Ibidem, , p.40.
[88] DONEDA, Danilo. Op. cit., p. 209.
[89] MENDES, Laura Schertel. Op. cit., p.40.
[90] Ibidem, p.40.

são colocados em xeque, uma vez que, se não disponibilizar seus dados, o cidadão pode ser excluído de algum aspecto da vida social ou ter algum prejuízo.

Uma terceira geração de leis é marcada pela decisão do Tribunal Constitucional Alemão de 1983 que, como já exposto, declarou o direito à autodeterminação informativa, radicalizando a ideia do controle dos cidadãos no processamento de dados. De acordo com Danilo Doneda[91], essa geração sofisticou a tutela de dados pessoais, que apesar de ainda ser centrada no cidadão, passava a abranger mais do que a liberdade de fornecer ou não seus dados pessoais - essa geração preocupava-se em garantir a efetividade desta liberdade.

A principal diferença dessa geração em relação á segunda é que as leis desse período procuravam fazer com que a pessoa participasse de maneira consciente e ativa em todo processo de tratamento e utilização de sua informação por terceiros. São exemplos as leis dos Estados alemães pós-decisão do Tribunal Constitucional, a emenda à Lei Federal de Proteção de Dados Pessoais alemã de 1990 e à da Lei de Áustria de 1986.

Entretanto, de forma análoga ao que ocorreu com a segunda geração de leis, a maioria dos cidadãos não estavam dispostos a arcar com os altos custos monetários e sociais de exercer o seu direito. Como analisa Danilo Doneda, a autodeterminação informativa "continuava sendo o privilégio de uma minoria que decidia enfrentar tais custos"[92].

E por fim surgiu a quarta geração de leis, como as que existem hoje em vários países. Essas leis buscaram resolver os problemas apresentados nos períodos anteriores por meio do fortalecimento da posição dos indivíduos. Um exemplo foi a previsão de reclamações individuais a respeito da violação da proteção de dados com a emenda da Lei Federal de Proteção de Dados da Alemanha[93].

Paradoxalmente, como apontam Doneda[94] e Mendes[95], essas leis também reduziram o papel de decisão individual em determinadas modalidades de dados, como os sensíveis, sob o raciocínio de que de tão relevantes, esses dados merecem ser extremamente protegidos, fora até da disposição individual dos cidadãos. Outra característica dessa geração é a complementação das leis gerais com normas setoriais específicas, como para o setor de crédito ou saúde.

---

[91] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 211.
[92] Ibidem, p. 212.
[93] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.43.
[94] DONEDA, Danilo. Op. cit., p. 212.
[95] MENDES, Laura Schertel. Op. cit. p.43.

Como pode ser visto, a disciplina da proteção de dados passou por uma série de transformações nas últimas décadas, principalmente em razão de diversas mudanças tecnológicas. A evolução dessas gerações parece demonstrar o fortalecimento do conceito de proteção da personalidade dos cidadãos[96] e uma tentativa de se buscar um modelo que de fato garanta a autodeterminação dos indivíduos.

Ao longo da evolução da proteção de dados pessoais, foi possível a consolidação de um regime jurídico de proteção de dados pessoais, com princípios e direitos comuns[97]. Um desses princípios é o consentimento, relacionado diretamente aos conceitos analisados de autodeterminação informativa e controle dos dados pessoais por parte dos cidadãos. Finda esta parte inicial de contextualização da sociedade em rede e economia da informação e demonstração do surgimento e evolução da proteção de dados, será analisado o papel do consentimento na disciplina de proteção dos dados pessoais. E em seguida, como ele é levado em consideração em duas normativas recentes: o Projeto brasileiro de Lei 5276/16 e o Regulamento Geral de Proteção de Dados Europeu, aprovado na União Europeia em 2016.

CAPÍTULO 2: O CONSENTIMENTO NA TUTELA DE DADOS PESSOAIS

2.1 O CONSENTIMENTO À LUZ DA AUTODETERMINAÇÃO INFORMATIVA E COMO FORMA DE LEGITIMAÇÃO DO TRATAMENTO DE DADOS PESSOAIS

No decorrer do desenvolvimento do conceito da privacidade como proteção de dados pessoais, foi estabelecido um consenso[98] em torno de um quadro básico de princípios norteadores do tratamento de dados por meio de instrumentos internacionais e transnacionais. Mesmo nos ordenamentos jurídicos mais diversos, há a previsão de praticamente os mesmos princípios de proteção de dados, com mínimas diferenças. A seguir serão apresentados alguns princípios básicos para, assim, ser apresentado o consentimento como um princípio de proteção de dados pessoais.

[96] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.44.
[97] Ibidem, p.44.
[98] Ibidem, p. 68.

Um princípio fundamental que todas as atividades de processamentos de dados devem seguir é o princípio da finalidade, que exige a correlação necessária entre o uso dos dados pessoais e a finalidade comunicada aos interessados no momento de coleta. Ele é uma forma de restrição da transferência de dados a terceiros[99] e é parâmetro para julgar se determinado uso de dados pessoais é adequado e razoável. O princípio da transparência ou publicidade exige que a existência de um banco de dados pessoais seja de conhecimento público, sendo uma forma de *accountability*. De acordo com ele, não podem existir bancos de dados sigilosos, sendo a transparência uma forma de se evitar o cometimento de abusos.

Outro princípio importante é o da qualidade de dados, que exige um tratamento leal e lícito aos dados constantes em um banco, bem como que esses dados sejam adequados, pertinentes e não excessivos em relação à finalidade declarada. Além disso, ele envolve a necessidade de dados sempre estarem exatos e atualizados. O princípio da segurança física e lógica exige a proteção de qualquer banco de dados contra extravios, destruições e desvios não autorizados pelos interessados. Próximo está o princípio da responsabilidade, que visa assegurar a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito de privacidade.

Finalmente, o princípio do consentimento é aquele que possibilita o controle do titular acerca de seus dados. Por meio do exercício do consentimento, o titular pode determinar um maior nível de proteção ou maior fluxo de seus dados, expressando – em tese - sua permissão, sua anuência, sua aprovação para certa forma de tratamento de dados pessoais. De acordo com esse princípio, o consentimento deve ser livre, específico e informado, sendo que apenas situações excepcionais previstas em lei justificariam o processamento de dados sem o prévio consentimento do titular, como defende Laura Schertel[100].

O consentimento é uma forma de implementar o direito à autodeterminação informativa, visto que envolve a própria participação do indivíduo, que funciona como uma mola propulsora[101] da estrutura da proteção de dados, permeando todo o processo de tratamento de dados. De acordo com a autora:

> Para que o indivíduo possa exercer o seu papel de autodeterminação informativa, faz-se necessário um instituto jurídico por meio do qual se expresse a sua vontade de

[99] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 216.
[100] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 71.
[101] DONEDA, Danilo. Op. cit., p. 212.

> autorizar ou não o processamento de dados pessoais: o consentimento. Este é o mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão.[102]

O consentimento surge como uma espécie de "carta coringa regulatória"[103] ao constituir um conjunto de autorizações e proibições[104] que regulam a atividade de tratamento de dados pessoais. A noção por detrás desse mecanismo é que os usuários façam escolhas conscientes, racionais e autônomas sobre o processamento de seus dados. Um pedido de consentimento deveria dar aos indivíduos uma pausa para fazê-los pensar a respeito das consequências envolvidas no tratamento daqueles dados[105].

O consentimento surge, então, como uma forma de autorizar, legitimar as técnicas de processamento e de dar algum poder de controle ao cidadão, de forma que ele não seja um mero "fornecedor de dados"[106]. E dessa forma, ele figura como um elemento central ao longo da evolução da proteção de dados pessoais, ao ponto desta proteção ser equiparada "ao direito do cidadão autogerenciar as suas informações pessoais"[107] .

Como foi visto no capítulo anterior, a depender do uso que se faz das técnicas de tratamento de dados, surgem riscos à privacidade dos usuários. Como o problema não está na técnica em si e sim no uso que se faz dela, o consentimento muitas vezes é visto como o modo de legitimar a técnica de tratamento de dados, na maioria das vezes acompanhado do princípio da informação e transparência.

Em se tratando da coleta de dados, sua legitimidade está condicionada ao consentimento ou não do cidadão ou à alguma previsão legal que permita sua coleta[108]. E isso se aplica tanto à coleta de dados a partir de transações comerciais, como de cartões de fidelidade, por exemplo, quanto à coleta de dados com o propósito de servir a censos e registros

---

[102] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 60.

[103] TENE & POLONETSKY, Apud BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[104] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 76.

[105] SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8, Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 Acesso em outubro de 2017.

[106] RODOTÀ, Stefano. Op. cit., p. 76.

[107] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[108] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 96.

públicos. Para que haja o consentimento, é necessária a informação ao usuário da finalidade da coleta de dados, bem como a transparência para que se demonstre que o dado não foi utilizado para além dessa finalidade. Quanto a pesquisas de mercado e de estilo de vida, por sua vez, é necessário que o realizador obtenha o consentimento do consumidor caso tenha interesse em compartilhar ou ceder tais dados a terceiros ou usar os dados como a finalidade de *marketing* direto.

Um exemplo sobre o consentimento na coleta de dados é o que ocorre, por exemplo, na compra *online* de um livro[109]. Assim que realiza o pedido, o indivíduo deve fornecer seu nome, endereço de entrega e detalhes sobre o pagamento para que complete a compra. Tal transação implica consentimento para o uso desses dados pessoais, geralmente consentimento com os termos gerais e condições do site. De acordo com vários desses termos, tal consentimento implica mais do que consentimento para entrega do pedido: ele inclui consentimento para customizar conteúdos e propagandas, para envio de e-mails, compartilhamento interno de dados comportamentais, pessoais e sua venda para terceiros.

No caso do processamento de dados[110], o consentimento também atua como forma de legitimar as técnicas, dados os riscos provenientes do uso de cada uma. No *data mining*, é importante que o usuário dê seu prévio consentimento para a mineração de dados, técnica que pode ser potencialmente discriminatória, à medida em que classifica as pessoas a partir de dados pessoais armazenados, possibilitando práticas que violem o princípio da igualdade. Nesse caso, a legitimidade da técnica pelo consentimento vem acompanhada estreitamente pelo princípio da informação e transparência no processamento de dados, de forma que o usuário seja informado do objetivo da coleta e de como seus dados serão processados.

No caso do *profiling*, uma vez que essa técnica possibilita a manipulação da vontade do usuário, bem como enseja o mau uso de dados de seu perfil, sua utilização depende do prévio consentimento do cidadão, bem como da possibilidade que ele tenha controle a respeito do perfil, por meio da correção e atualização de suas informações. O mesmo vale para o *scoring:* dado o caráter potencialmente discriminatório dessa técnica, o indivíduo deve ser informado

[109] SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8, Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 Acesso em outubro de 2017.

[110] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.107.

para que consinta com o uso desse sistema de avaliação. Esse consentimento precisa vir acompanhado da informação e transparência aos usuários.

O consentimento, no decorrer das gerações de leis de proteção de dados pessoais, sempre adquiriu um papel de centralidade[111], com menor ou maior carga participativa do indivíduo em autodeterminar as suas informações pessoais.

Essa carga participativa maior ou menor está relacionada à sua adjetivação, isto é, ao conjunto de adjetivos que o acompanham, como "informado", "livre" e "expresso". Tais aspectos, vitais para a validade do consentimento, serão melhor analisados mais à frente e ajudarão na compreensão de como funcionalizar esse mecanismo.

E além disso, será investigada também essa própria centralidade do consentimento, que vem sendo questionada a partir da constante inovação nos modelos de negócio da economia digital que têm nos dados pessoais a sua base de sustentação[112]. Mas antes, faz-se necessário considerar qual seria a natureza jurídica desse mecanismo de autodeterminação informacional.

2.2. A NATUREZA DO CONSENTIMENTO

Nos termos do art. 4º item 11 do Regulamento Geral de Proteção de Dados, consentimento é uma "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". Como definiu Laura Schertel, ele é o "mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão" [113].

Segundo Orlando Gomes, o consentimento é um típico elemento do direito contratual, "por meio do qual que os indivíduos exprimem a sua vontade de contratar, dando ciência uma a outra da sua intenção negocial para que seja selado um compromisso entre

[111] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.
[112] Ibidem, p. 28.
[113] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 60.

elas"[114]. Mas dentro de um contexto de proteção de dados pessoais, a qualificação do consentimento não é tão simples assim, como afirma Danilo Doneda:

> A qualificação jurídica do consentimento para o tratamento de dados pessoais não deve ser tomada como um mero enquadramento da sua disciplina em um esquema preconcebido, pelo qual o tratamento de dados deva submeter-se aos cânones de uma determinada concepção da autonomia privada. A especificidade do consentimento para o tratamento de dados pessoais pede uma funcionalização de sua própria natureza jurídica, e ao intérprete cabe integrar esta disciplina do consentimento com os efeitos que dela são pretendidos[115].

Na verdade, a natureza do consentimento no âmbito do tratamento de dados pessoas é um tema que gera bastante polêmica. De acordo com Schertel[116], existem três principais correntes: i) a primeira entende que o consentimento para o processamento de dados tem natureza de uma declaração de vontade negocial; ii) a segunda entende que se trata de um ato jurídico unilateral sem natureza negocial; e iii) a terceira entende que o consentimento é um ato que se assemelha ao negócio jurídico sem o ser.

Danilo Doneda entende não ser apropriado atribuir uma natureza negocial ao consentimento por se tratar de um mecanismo que toca diretamente elementos da própria personalidade, mas sem dispor destes elementos[117]. Para ele, considerar o consentimento a partir de uma natureza negocial seria inseri-lo numa estrutura contratual, o que acarretaria a utilização de esquemas proprietários para o tratamento de dados pessoais e dificultaria a atuação dos atributos da personalidade:

> Assim, justifica-se a não consideração deste consentimento como um negócio jurídico, já que esta opção reforçaria o sinalagma entre o consentimento para o tratamento dos dados pessoais e uma determinada vantagem obtida por aquele que consente, reforçando a sua índole contratual e, consequentemente, acarretando a utilização de esquemas proprietários para o tratamento de dados pessoais[118].

Para o autor, o consentimento assume as vestes de um ato unilateral, "cujo efeito é o de autorizar um determinado tratamento para os dados pessoais, sem estar diretamente vinculado a uma estrutura contratual"[119], o que aproxima Doneda da segunda corrente.

---

[114] GOMES, Orlando. Contratos. 26. ed. 2ª tiragem. Rio de Janeiro: Forense, 2008 Apud. BIONI, Bruno. XEQUE-MATE. O Tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. USP- Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, 2016.
[115] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 377.
[116] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 62.
[117] DONEDA, Danilo. Op. cit., P. 377.
[118] Ibidem, p. 379.
[119] Ibidem, p. 378.

Já Laura S. Mendes entende que o último posicionamento é atualmente o dominante e o mais correto, uma vez que o consentimento possui sim características negociais, mas ao mesmo tempo tem caráter personalíssimo, adquirindo uma natureza que ela chama de "atípica"[120]. Por causa dessa natureza diferenciada, a autora aponta que para decidir quais são as normas aplicáveis ao consentimento, é preciso uma análise caso a caso.

A função do consentimento para a tutela de dados pessoais seria a mesma da declaração de vontade no âmbito de um negócio jurídico, visto que ambos visam à autodeterminação da pessoa. Por tal motivo, seria possível a aplicação das regras referentes aos negócios jurídicos e contratos em geral a esse consentimento, sempre que essa aplicação "mostrar-se cabível e adequada"[121].

Por outro lado, a autora coloca um exemplo de quando uma norma não seria aplicável. O exemplo é o relacionado à capacidade civil[122]. Uma vez que o caráter personalíssimo do consentimento para o processamento de dados se sobressai, o fundamental é identificar se a pessoa tem capacidade de discernimento para autorizar determinado tipo de coleta ou tratamento de dados, não sendo necessária a capacidade civil para tanto. As autoridades alemãs de proteção de dados, por exemplo, diante da ausência de normas a esse respeito, entendem que a partir dos 14 anos completos, a pessoa já teria condições para consentir a respeito do processamento de dados pessoais[123].

Apesar das diferenças de posicionamento, ambos os autores concordam que há um problema na compreensão dos perfis do consentimento: de um lado, o perfil ligado ao caráter personalíssimo e do outro, o ligado à utilidade dos dados. Laura Schertel reconhece as características negociais do consentimento e seu caráter personalíssimo, optando por uma estrutura atípica – ato que se assemelha ao negócio jurídico sem o ser.

---

[120] MENDES, Laura Schertel. Op. cit., p. 63.
[121] Ibidem, p. 63.
[122] Arts. 3º e 4º do Código Civil.
[123] Agora, com a edição do Regulamento Europeu que entra em vigor em maio de 2018, há um artigo dedicado a isso:
"Artigo 8º - Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação. 1. Quando for aplicável o artigo 6º, nº1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança. Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos. 2. Nesses casos, o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível. 3. O disposto no nº1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança".

Mas a despeito de afastar a ideia negocial do consentimento, Doneda também admite que, ao passo que o consentimento é o instrumento por excelência da autodeterminação e tutela da pessoa, ele é também uma forma de legitimação para que os dados pessoais sejam, em alguma medida, utilizados por terceiros, significando "a transformação destes dados em uma determinada utilidade"[124].

Sendo assim, apesar de afastar o consentimento da natureza de negócio jurídico, por ser esse mecanismo uma "condição de acesso"[125] para a vida privada ligada ao poder de autodeterminação, Danilo Doneda ainda percebe o consentimento como uma forma de legitimar a inserção dos dados pessoais no mercado, o que o faz reconhecer a necessidade de equilíbrio entre ambos os perfis – o que de pronto[126] já admite não se tratar de uma tarefa simples.

2.3 O PARADOXO DA PRIVACIDADE

Apesar da relevância desse mecanismo no âmbito da proteção de dados pessoais, ainda existe uma questão relevante a respeito do consentimento, de certa forma ligado à sua natureza, levantada por Danilo Doneda:

> Na medida em que o consentimento do indivíduo permite o processamento dos seus dados, na eventual hipótese de violação ao seu direito de privacidade, como poderia ele reivindicar a reparação daquela violação, se tinha autorizado o tratamento de seus dados pessoais?[127]

É o que o autor chama de "paradoxo da privacidade"[128], porque a estrutura desse direito exige, em tese, que primeiramente o indivíduo autorize o processamento de seus dados, para que só depois busque a sua tutela jurídica. Quando o consentimento centraliza a disciplina do processamento de dados pessoais, o interessado pode obter a tutela somente em um momento posterior a este consentimento, valendo-se do questionamento de algum defeito deste. Isso implica que a pessoa tenha que, primeiro, consentir em revelar seus dados para somente depois se valer da tutela[129].

[124] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 378.
[125] Ibidem, p. 379.
[126] Ibidem, p. 379.
[127] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 61.
[128] DONEDA, Danilo. Op. cit., p. 374.
[129] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 375.

Dessa forma, se for considerada a função inicial do consentimento como um instrumento para a livre construção da esfera privada, esse consentimento seria apenas uma ficção:

> Sua utilização pode ser instrumentalizada pelos interesses que pretendem que a sua disciplina não seja mais que uma via para legitimar a inserção dos dados pessoais no mercado. Ou então um determinado perfil do consentimento pode ser incentivado pelo próprio Estado sob a (falsa) premissa de conceder aos cidadãos um forte instrumento para determinar livremente a utilização de seus próprios dados pessoais – conforme observou Stefano Rodotà, o Estado assim teria um falso álibi para não intervir em uma situação na qual sua obrigação seria a de agir positivamente na defesa de direitos fundamentais – e, assim, "lavaria as mãos"[130].

Entretanto, para a resolução dessa questão, é importante entender que, como já exposto, o consentimento não representa a ausência de interesse do indivíduo na tutela de dados pessoais, mas um ato de escolha no âmbito da autodeterminação individual. E esse exercício está muito mais na possibilidade de concedê-lo ou negá-lo, neste poder de conceder ou negar, do que no momento do consentimento em si. Sendo assim, não é o consentimento em si que transmuda a informação pessoal em um bem jurídico[131].

A fundamentação do consentimento, portanto, reside na possibilidade de autodeterminação em relação aos dados pessoais, e ela deve ser levada em conta como elemento principal para a caracterização tanto da natureza jurídica do consentimento como para os efeitos desse consentimento.

2.4. PRESSUPOSTOS PARA UM CONSENTIMENTO VÁLIDO: OS ADJETIVOS DO CONSENTIMENTO

A problemática do consentimento gira em torno de como essa forma de controle deve ganhar vida. Pode-se dizer, como afirma Laura Schertel[132], que existem alguns pressupostos para a validade do consentimento, a saber: i) o titular deve emitir consentimento por sua livre e espontânea vontade; ii) o consentimento deve ser voltado a uma finalidade específica; iii) deve haver informação ao usuário sobre os objetivos da coleta, processamento e uso de dados e consequências sobre o não consentir com o tratamento. No mesmo sentido,

[130] Ibidem, p. 375.
[131] Ibidem, p. 378.
[132] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 65.

Doneda afirma que para sua funcionalização, não há como imaginar o consentimento sem antes considerar alguns dos princípios como finalidade e informação[133].

Para outros autores como Bart W. Schermer, Bart Custers e Simone van der Hof da Universidade de Leiden[134], é necessário que o consentimento seja dado por um sujeito com entendimento substancial acerca das consequências daquela manifestação de vontade, além de que essa manifestação seja intencional, livre de coerção, e que autorize um processo específico.

Dessa forma, para que o consentimento seja considerado válido, existem alguns critérios a serem preenchidos. A esse conjunto de critérios, quando da elaboração normativa, dá-se o nome de "adjetivação do consentimento". A exemplo do art. 4º item 11 do Regulamento Geral de Proteção de Dados[135], o consentimento deve ser livre, específico, informado, explícito e inequívoco. O PL 5276/16, por exemplo, fala sobre uma "finalidade determinada" em seu art. 5º, VII[136].

Assim como foi visto na seção anterior, em que o consentimento pode assumir várias roupagens em termos de sua natureza jurídica, ele também pode cercar-se de vários adjetivos, tais como informado, livre, com finalidade determinada, inequívoco, expresso e específico. Existiriam alguns adjetivos vitais para a validade do consentimento, e "informado" é um deles. Em boa parte da doutrina, inclusive, fala-se em "*informed consent*", e muitas vezes o termo consentimento é utilizado no próprio lugar de "consentimento informado"[137]. Agora outros como "expresso" não estão presentes como o "informado" em várias legislações que versam sobre o assunto.

Não há um consenso na doutrina acerca de quais adjetivos específicos devem ser abordados pelas normativas que tratem sobre a tutela de dados pessoais. Há aquelas expressões que se repetem e acabam por formar um "quadro comum"[138] nas diversas legislações.

---

[133] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 382.
[134] SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8, Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 Acesso em outubro de 2017.
[135] Nos termos do art. 4º item 11 do Regulamento (UE) 2016/679, consentimento é uma "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".
[136] "Art. 5º. Para os fins desta lei considera-se: VII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados para uma finalidade determinada"
[137] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.
[138] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 68.

Considerando que o consentimento é um instrumento de controle e autodeterminação, chegou-se à ideia de que a depender da extensão de sua adjetivação, pode haver uma carga menor ou maior de participação do titular de dados. Para fins de sistematização, em uma análise comparativa de projetos de leis brasileiros sobre proteção de dados intitulado "Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil"[139], elaborado por Bruno Bioni, foi criada uma "abordagem escalável" do consentimento que busca estabelecer uma análise progressiva de sua adjetivação.

O quadro utilizado no relatório é bem elucidativo para relacionar a escalada da adjetivação do consentimento e sua respectiva carga participativa para o titular dos dados pessoais[140]:

ESCALADA PROGRESSIVA DA ADJETIVAÇÃO DO CONSENTIMENTO E A CORRESPONDENTE CARGA PARTICIPATIVA DO TITULAR DOS DADOS PESSOAIS

ADJETIVOS DOS CONSENTIMENTO	CARGA DE PARTICIPAÇÃO
Expresso e Específico	Máxima
Inequívoco	Intermediária
Finalidade determinada	Pré-intermediária
Livre	Mínima
Informado	Básica

Como já mencionado, o quadro acima foi elaborado com o propósito específico de se comparar a adjetivação do consentimento nas principais iniciativas legislativas no Brasil. E como foi dito, não há um consenso na doutrina acerca de quais adjetivos devem ser abordados pelas legislações de proteção de dados pessoais, apenas um "quadro comum". Neste trabalho, adotou-se tal abordagem escalável apenas como um norte para a seguinte explicitação dos pressupostos para que o consentimento seja legítimo.

[139] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[140] Quadro 6 - Fonte: BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf

INFORMADO

Segundo a abordagem escalável elaborada por Bruno Bioni[141], o consentimento informado seria aquele com a carga básica de participação. Ele é "a porta de entrada (pressuposto) para que o cidadão ingresse (tenha participação) dentro da dinâmica de proteção dos dados pessoais, viabilizando-se, em última análise, a racionalização de um processo de tomada de decisão a seu respeito"[142].

De fato, como foi visto no início do capítulo, o poder de controle relacionado ao consentimento é na maioria das vezes atrelado à informação. Em boa parte da doutrina, o termo consentimento é utilizado no próprio lugar de "consentimento informado"[143], compreendendo uma série de disposições que prescrevem quais devem ser as informações fornecidas ao interessado para que seu consentimento seja válido ou não[144].

Ele carrega uma noção baseada na autodeterminação informativa, de forma a respeitar os usuários como centros individuais de controle sobre suas próprias vidas[145]. Ele envolve que a pessoa a quem é pedido o consentimento tenha sido devidamente informada do que ela está consentindo, de forma que ela esteja ciente das consequências e riscos daquela decisão. Assim, ele é uma forma de garantir, em tese, decisões racionais, bem consideradas e avaliadas[146]. E como decorrência disso, a ausência de consentimento pode implicar numa violação ao princípio da autonomia[147].

O modelo básico de consentimento consiste em dois passos[148], a saber (1) o pedido de consentimento de um controlador de dados e (2) o fornecimento ou não de consentimento pelo usuário. Olhando de perto esses dois passos, é possível perceber uma série de ações em cada um. O primeiro passo envolve, por exemplo, que o controlador de dados disponibilize informações necessárias para que o usuário esteja apto a tomar uma decisão. Essas informações

---

[141] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.
[142] Ibidem, p. 28.
[143] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. P. 2. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.
[144] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 78.
[145] CUSTERS B.H.M., HOF S. van der; SCHERMER B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy and Interne, 2014. P. 268-295. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163 Acesso em outubro de 2017.
[146] CUSTERS, Bart. Op. cit., p. 2.
[147]CUSTERS B.H.M., HOF S. van der; SCHERMER B. (2014). Op. cit. P. 268-295. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163 Acesso em outubro de 2017.
[148] Ibidem, p. 268-295.

devem referir-se tanto ao conteúdo do consentimento (a que exatamente o consentimento está senso dado) como ao processo (como consentir).

A informação sobre o conteúdo do consentimento pode incluir detalhes acerca de quais dados pessoais estão sendo coletados e para quais finalidades. Pode incluir também as consequências do consentimento, como direitos e obrigações decorrentes para o usuário que consente. A informação sobre como consentir pode dizer respeito à forma em si, como se clicando em uma caixa ou submetendo um formulário, e à possibilidade de revogação do consentimento.

Já o segundo passo, aquele que consiste em fornecer o consentimento, envolve que o usuário forneça informações sobre o conteúdo (foi dado o consentimento ou não? Para quais partes? Há alguma condição particular?) e sobre ele mesmo (identidade do usuário e informações a mais, como sua idade, ou detalhes sobre cartão de crédito).

Para uma ilustração sobre como seria a avaliação de um consentimento informado ou não, é interessante analisar os critérios elaborados por Bart Custers, Simone van der Hof e Bart Schermer com os principais quesitos para determinar a existência de um consentimento informado[149]. A tabela foi fruto de um estudo que comparava as práticas nas redes sociais que envolvem o consentimento informado e as expectativas dos usuários sobre esse instituto jurídico, com base nas previsões legais da proteção de dados da União Europeia e literatura. A distinção é feita com base em dois focos principais: o próprio consentimento (quem dá o consentimento e como isso é realizado) e as condições (que informações devem ser disponibilizadas e como)[150]:

Critérios sobre a decisão de consentir	A pessoa que consente	A pessoa que consente é adulta? Caso contrário, há consentimento dos pais?
		A pessoa que consente é capaz? Caso contrário, há consentimento dos representantes legais?
		A pessoa que consente é competente para consentir?
		O consentimento é escrito?

[149] CUSTERS B.H.M., HOF S. van der; SCHERMER B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy and Interne, 2014. P. 268-295. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163 Acesso em outubro de 2017

[150] Fonte: Tradução livre da tabela 1, p. 438. CUSTERS B.H.M., HOF S. van der, SCHERMER B.W., APPLEBY-ARNOLD S., BROCKDORFF & N. Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, Scripted: A Journal of Law and Technology, 2013. P. 435-457. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134 Acesso em outubro de 2017.

	Como é fornecido o consentimento	O consentimento é parcial ou completo? No caso de ser parcial, ele é suficiente para a finalidade comunicada?
		O consentimento é razoavelmente forte?
		O consentimento é fruto de uma decisão independente?
		O consentimento é atualizado?
Critérios sobre o discernimento na decisão do consentimento	Quais informações devem ser disponibilizadas ao usuário	Está claro como os dados são coletados, usados e compartilhados?
		As propostas são claras?
		As medidas de segurança são claras?
		Está claro quem é o responsável por processar os dados?
		Estão claros quais direitos podem ser exercidos e de que forma?
	Como as informações devem ser disponibilizadas ao usuário	A informação é específica e suficientemente detalhada?
		A informação é compreensível?
		A informação é acurada e confiável?
		A informação é acessível?

Para a análise do presente trabalho, interessante observar que dentre as informações que devem ser disponibilizados ao usuário, constam a clareza sobre como os dados serão coletados, usados e compartilhados, bem como quem será o responsável por esse processamento de dados e quais as medidas de segurança envolvidas.

Não basta apenas informar. Essa informação disponibilizada ao usuário deve ser específica, detalhada, compreensível, acurada, confiável e acessível. Somente dessa forma é possível imaginar que o cidadão tenha instrumentos suficientes para tomar uma decisão informada e consciente.

LIVRE

O consentimento livre dentro da abordagem escalável encontra-se como uma forma mínima de carga participativa do cidadão na tutela de seus dados pessoais. Livre diz respeito a uma manifestação de vontade que não é fruto de nenhuma coação, seja ela física ou moral. É necessário que o usuário emita o consentimento por sua livre vontade.

Schermer, Custers e van der Hof[151] denominam esse aspecto como a ausência de coerção por terceiros. Para que o consentimento seja válido, ele deve ser oferecido de maneira livre, como resultado de uma escolha autônoma por aquele que consente. A ausência de controle por terceiros no momento do consentimento pressupõe um elemento de escolha: se recusar o consentimento não é uma escolha viável, ou por ser impossível, ou por trazer um impacto muito negativo ao titular dos dados, então não há escolha real e, portanto, não há consentimento. Da mesma forma, se a pessoa está sob qualquer outra forma de influência devida, o consentimento está viciado.

Um exemplo de situação em que o consentimento pode ser questionado é o de, quando no contexto de uma relação laboral, a situação de subordinação do empregado tende a minar a voluntariedade do consentimento, especialmente quando a não autorização pode resultar em uma demissão[152]. Laura Schertel também aponta para outra relação de assimetria de poder, além da trabalhista, como a relação de consumo, reforçando a necessidade de uma análise caso a caso para verificar se o consentimento de fato é dado de forma livre ou não passa de uma mera ficção[153].

FINALIDADE DETERMINADA

Ainda consoante à abordagem escalável, essa seria uma forma de participação pré-intermediária do titular de dados pessoais. Muito relacionado ao dever de informação, é importante que o consentimento seja voltado a uma finalidade específica. Isso significa dizer que essa manifestação de vontade do titular deve ter um direcionamento, não pode ser feita com base em propósitos totalmente genéricos, sob o perigo de o titular dos dados emitir uma espécie de "cheque em branco"[154].

---

[151] SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 Acesso em outubro de 2017.

[152] Exemplo utilizado pelo Relatório ao caracterizar o adjetivo "livre". BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[153] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 65.

[154] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

Por outro lado, Bruno Bioni mostra outro sentido da expressão "finalidade determinada":

> Ao mesmo tempo, a locução "finalidade determinada" abre margem para que o ato de consentir não desça a descrições tão restritas, mas a um leque de situações que façam sentido dentro de um determinado contexto (...) Por exemplo, em serviços de *internet banking* seria razoável que os dados pessoais dos consumidores fossem tratados não só para operacionalizar o próprio serviço em si de transferências financeiras, como, também, para prevenção de fraudes. Tais finalidades são determinadas de acordo com o escopo da relação em questão[155].

INEQUÍVOCO

Essa seria uma forma intermediária de participação do cidadão, consistindo numa hipótese de consentimento tácito, um conjunto de autorizações subentendidas pelo contexto da relação na qual fluem os dados[156]. Na esteira do exemplo dado por Bruno Bioni dos serviços de *internet banking,* em que a autorização para o tratamento dos dados seria feita também para a prevenção de fraudes, o adjetivo "inequívoco" seria uma forma de autorização subentendida.

Uma classificação dentro do consentimento inequívoco, seria o implícito - que diria respeito a uma omissão ou passividade que produz efeitos, uma dedução inequívoca de intenção- , ou explícito, que seria uma manifestação ativa. De acordo com o que já foi exposto, uma autorização tácita e passiva, ainda mais quando não devidamente informada, parece minar o conceito de autodeterminação informacional.

Nesse sentido, entra uma questão controversa acerca dos "interesses legítimos". Esse é um conceito presente tanto no PL 5276/16 quanto no novo Regulamento Geral de Proteção de Dados para autorizar determinadas situações nas quais o consentimento não precisaria ser emitido. São situações em que não seria necessário perguntar ao cidadão se o tratamento pode ser realizado, porque ele deveria contemplar as suas "legítimas expectativas"[157]. O ponto será melhor analisado em momento oportuno no terceiro capítulo, em que será observado com maior detalhe a disposição do consentimento nas duas disposições normativas.

---

[155] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[156] Ibidem, p. 29.

[157] http://www.internetlab.org.br/pt/opiniao/especial-o-que-pode-autorizar-o-tratamento-de-dados-pessoais/ Acesso em novembro de 2017.

ESPECÍFICO E EXPRESSO

Por fim, esses dois últimos adjetivos estariam relacionados à carga máxima de participação do cidadão no tratamento de seus dados pessoais. Schermer, Custers e van der Hof[158] tratam desses adjetivos como "autorização do curso de ação" ou especificidade. De acordo com essa definição, o titular consente com todo o processo pelo qual os seus dados serão tratados. E nesse sentido, é necessário que esse processo seja claro – remetendo ao consentimento informado -, sob o risco de um consentimento fraco, com grande margem interpretativa e incertezas para o titular dos dados pessoais.

De forma diversa ao sentido dado por Bruno Bioni à "finalidade determinada", o consentimento adjetivado pelo termo "específico" deve detalhar todo o processo pelo qual os dados serão tratados, o que conferiria ao titular um maior controle sobre os seus dados, em todo o seu movimento. Diferentemente da adjetivação "para finalidade determinada" e do qualificador "inequívoco", "específico e expresso" seriam adjetivações que potencializariam ao máximo a autodeterminação informacional dos cidadãos, afastando "qualquer tipo de autorização passiva, tácita ou implícita"[159] por parte do usuário.

De acordo com o relatório que compara as iniciativas legislativas brasileiras, sob o ponto de vista da técnica legislativa e com base na escala progressiva sistematizada, seria mais coerente em termos normativos "a utilização do termo específico vir sempre acompanhado do termo expresso, por serem duas faces da mesma moeda que simbolizam a potência máxima da autodeterminação informacional" [160].

2.5. POSSIBILIDADE DE REVOGAÇÃO E RENOVAÇÃO DO CONSENTIMENTO

Tendo em vista a necessidade de pressupostos para um consentimento válido e sua extensa adjetivação como forma de conferir legitimidade e maior participação do cidadão no

[158] SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 Acesso em outubro de 2017.

[159] Internetlab. O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais? Disponível em: < http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de--lei-de-protecao-de-dados-pessoais/> Acesso em novembro de 2017.

[160] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 48. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

processo de tratamento de dados, adquire grande relevância a possibilidade de revogação do consentimento como forma de fazer valer a autodeterminação dos indivíduos.

A ideia da revogabilidade do consentimento encontra fundamento no fato de que seria uma proteção à própria personalidade, sendo a indisponibilidade um de seus atributos[161]. Tal concepção, segundo Danilo Doneda, liga-se diretamente à atribuição da natureza de ato jurídico a ao consentimento: "no exercício desta autodeterminação, o sujeito não está constrito a efeitos vinculantes de natureza obrigacional resultantes de seu consentimento – e, consequentemente, não se pode associar tal ato a um inadimplemento de qualquer espécie"[162]. Segundo o autor, a própria caracterização do consentimento como ato jurídico unilateral reforça a sua revogabilidade.

Uma questão que fica em aberto, do outro lado do exercício do livre desenvolvimento da personalidade, seria a situação de quem recebeu a autorização para o tratamento de dados pessoais: se o outro lado arcaria com todo o risco decorrente da revogação do consentimento. Doneda comenta que este risco "pertence à intrínseca natureza de sua posição e é justificável na medida em que o seu interesse e a utilidade que busca provém do tratamento dos referidos dados pessoais"[163].

Nessa seara, Laura Schertel utiliza como exemplo o ordenamento espanhol e o alemão que já preveem a revogabilidade do consentimento. No caso espanhol, a revogação do consentimento exige uma causa justificada, ou seja, aquela relacionada ao descumprimento de obrigações por parte do responsável pelo tratamento de dados pessoais, e não pode acarretar efeitos retroativos. Já com relação à cessão de dados, nem é necessária justificativa, tendo em vista a ameaça maior à personalidade do cidadão[164].

No caso alemão, o consentimento sempre pode ser revogado sem a necessidade de justificativa, sendo tratado como uma forma de controle não apenas preventivo, como também posterior, caso o titular de dados avalie que o tratamento de dados não está mais adequado ou atendendo aos seus interesses.

Para a autora, dogmaticamente falando, a possibilidade de revogação do consentimento sem justificativa parece ser a mais adequada, tendo em vista que seria inerente ao próprio direito da personalidade, sendo o consentimento a forma de proteção dos dados

[161] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 61.
[162] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 380.
[163] Ibidem, p.380.
[164] MENDES, Laura Schertel. Op. cit., p. 64.

pessoais. Segundo ela, "a própria dificuldade que o indivíduo enfrenta para visualizar e avaliar as consequências do seu consentimento no início do processo de tratamento de dados justificaria a livre possibilidade de revogação do consentimento"[165].

Da mesma forma, fala-se na possibilidade de renovação do consentimento como o "direito de mudar de ideia"[166]. Muitos sites, como por exemplo aqueles relacionados a redes sociais, notificam os usuários acerca de mudanças em sua política de privacidade, mas não perguntam expressamente sobre a renovação do consentimento. O que leva Bast Custers a intitular seu artigo "*Click here to consent forever*", ao tratar sobre o tema:

> "(...) o consentimento é geralmente solicitado quando do registro, mas raramente é renovado. Como resultado, consentir uma vez implica em consentir para sempre. Ao mesmo tempo, dadas às rápidas transformações no Big Data e análise de dados, o consentimento pode facilmente tornar-se desatualizado (quando o consentimento anterior não mais reflete as preferências dos usuários)" [167]

O autor propõe a possibilidade de datas para o expirar do consentimento, considerando que ele deve contemplar o atual processo de tratamento de dados. E por tal motivo, é importante que o consentimento seja atualizado. Apesar de indicar a ausência dessa previsão no Regulamento Europeu, o autor argumenta que tal implicação pode ser retirada da própria adjetivação do consentimento: se o tutelar dos dados consentiu para uma finalidade específica, qualquer desvio substancial dessa finalidade deve requerer uma renovação ou confirmação do consentimento.

Custers demonstra que muitos serviços que utilizam as redes e dados como forma de sustentação econômica argumentam que a qualquer momento o consentimento pode ser revogado. Inclusive é o que consta no novo Regulamento EU, item 3 de seu art. 7º:

> O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular

---

[165] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 65.

[166] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.

[167] Tradução livre do seguinte trecho: *"(...) consent is usually asked for when registering, but rarely is consent renewed. As a result, consenting once often implies consent forever. At the same time, given the rapid changes in Big Data and data analysis, consent may easily get outdated (when earlier consent no longer reflects a user's preferences)".* CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.

> dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.

Contudo, ele apresenta alguns problemas para esse argumento. Primeiro, ele leva à uma mentalidade "*take it or leave it*": discordar com certos termos novos significa não ter mais acesso ao site ou serviço, completa ou parcialmente. Além disso, muitos usuários podem não querer cancelar suas contas grátis, sendo muito mais propensos a apenas abandonar o serviço. Entretanto, os controladores dos dados continuam a usar seus dados pessoais. Diante disso, o autor propõe um limite máximo de tempo para a duração do consentimento - caso não renovado, o consentimento expiraria depois de 2 ou 3 anos, por exemplo.

O artigo defende que, quando perguntados regularmente sobre a possibilidade de renovar seu consentimento, aqueles usuários mais engajados poderiam se aperceber que mudaram de ideia no decorrer do tempo e que mudaram as formas de processamento de dados. Além disso, as pessoas poderiam entender melhor as consequências de seu consentimento após usarem o site ou serviço por um tempo do que à época de registro.

Longe de apontar essa forma de consentimento como uma solução a ser adotada e sim como uma forma de início de debate acerca do assunto, o autor coloca também algumas questões práticas: assim que a data do consentimento expirasse, nada impediria o uso dos dados anonimizados, uma vez que a proteção de dados pessoais se refere, como foi visto, aos dados relacionados a pessoas identificadas ou identificáveis. Assim, "consentimento expirável" não resolveria como um todo o problema.

Ademais, uma das questões que ainda não estariam resolvidas com essa proposta seria a de que esse consentimento tomaria a mesma forma que o consentimento inicial, o que, como será exposto adiante, é atualmente um problema. Para muitos, pode ser apenas mais uma caixa de diálogo a se clicar. Outra questão seria a não exclusão dos dados pessoais pelos controladores após a "data de validade" do consentimento.

Apesar de admitir não solucionar esses dilemas, o autor coloca que a proposta ainda poderia ser útil para aqueles usuários que estão há muito sem utilizar um site ou serviço. A inatividade poderia ser automaticamente interpretada como uma revogação do consentimento, bloqueando o uso futuro de seus dados pessoais, como uma forma de proteção ao tutelar de dados.

2.6. AS CRÍTICAS AO CONSENTIMENTO: DIFICULDADES E DESAFIOS

Como foi visto até o momento, o consentimento é um importante instrumento para o controle do titular no contexto de proteção de dados pessoais e uma forma de exercício do que se chama autodeterminação informacional. Não é à toa que ele é o pilar normativo da grande maioria das leis ao redor do mundo, senão de todas elas[168], ocupando um papel central na proteção de dados pessoais por várias gerações de leis.

Contudo, essa realidade parece ter sido alterada. Fala-se atualmente na "crise do consentimento"[169]. Já é pacífico na doutrina[170] que o papel do consentimento na proteção de dados pessoais tem mudado e, aos poucos, perdido sua centralidade. Mas para um melhor entendimento de como se chegou nessa situação, é importante analisar como tem sido a implementação do consentimento como forma de proteção de dados pessoais – se efetiva ou não - e algumas críticas que têm sido feitas em decorrência disso.

No contexto de Big Data, tem sido crescente o ceticismo acerca da efetividade do consentimento na proteção de dados pessoais. No que diz respeito aos modelos de consentimento baseados na autodeterminação informacional, Solove[171] argumenta que tais modelos têm falhado em oferecer uma proteção adequada aos cidadãos, uma vez que apresentam diversos obstáculos, a saber: (1) as pessoas não leem as políticas de privacidade; (2) se as pessoas leem, elas não entendem tais políticas; (3) se as pessoas leem e entendem as políticas de privacidade, elas geralmente não possuem um conhecimento prévio para tomar uma decisão informada; (4) se as pessoas leem as políticas de privacidade, as entendem e são aptas a tomar uma decisão informada, geralmente não são oferecidas a elas as escolhas que melhor definem suas preferências.

Quando o consentimento é solicitado, as informações oferecidas geralmente são muito extensas, demandando um bom tempo do usuário para leitura e ponderamento na tomada

[168]BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[169] SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology. DOI: 10.1007/s10676-014-9343-8, Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418 Acesso em outubro de 2017.

[170] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128.Acesso em outubro de 2017.

[171] SOLOVE, DJ (2013) Privacy self-management and the consent dilemma. Harvard Law Review 126: 1880–1903. Disponível em: https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/ Acesso em novembro de 2017.

de uma decisão. Como estimado por McDonald e Cranor[172], se os usuários fossem de fato ler todas as políticas de privacidade que lhe são apresentadas, isso levaria nada menos 244 horas anualmente.

Já existem pesquisas indicando que as pessoas geralmente não leem as políticas de privacidade. Os motivos são vários. As informações fornecidas geralmente são de difícil compreensão. Em várias situações, texto é de natureza altamente jurídica e contém detalhes técnicos que vão além da capacidade de conhecimento da média dos usuários[173].

De acordo com um estudo elaborado por Bart Custers, Simone van der Hof e Bart Schermer na Universidade de Leiden em 2014[174], essas tendências puderam ser comprovadas. Na pesquisa, foi feita uma comparação entre as práticas que envolviam consentimento para o uso de dados pessoais e as expectativas dos usuários a respeito da privacidade e do consentimento. A comparação foi feita com base em vários critérios colhidos na literatura. A tabela utilizada na seção "consentimento informado" deste presente trabalho é, inclusive, o resultado da compilação desses quesitos.

Após o levantamento desses critérios para a pesquisa, foram selecionados 8 sites relacionados a redes sociais tais como *Youtube*, *Facebook*, *Twitter* e *Wikipedia*, e sites que demandam dados pessoais, para que fosse feita uma análise com base naquele conjunto de critérios para um consentimento informado. Por outro lado, foram colhidos dados acerca das expectativas de 8621 usuários ao longo de 26 países da União Europeia.

Perguntas foram feitas aos entrevistados, tais como "quando você cria uma conta em um site que nunca utilizou antes, você costuma ler as políticas de privacidade?" , "você observa os modos de controle de privacidade do que você recebe online, como *'check boxes'* que te permitem uma escolha *opt-in* ou *opt-out* de determinadas ofertas?" e "você já alterou alguma condição de privacidade no seu perfil pessoal em sites de redes sociais?". 73% respondeu que nunca, raramente ou às vezes lia as políticas de privacidade. 37,5% dos entrevistados sempre conferiam os "*check boxes*" e 29,9% já tinha alterado condições de privacidade em seu perfil pessoal.

---

[172] MCDONALD, A.M. ; CRANOR LF. The cost of reading privacy policies. I/S Journal for Law and Policy for the Information Society. 2008, Privacy Year in Review, 2008. Disponível em: <http://www.aleecia.com/authors-drafts/ reading. PolicyCost-AV.pdf.>. Acesso em novembro de 2017

[173] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.

[174] CUSTERS B.H.M., HOF S. van der; SCHERMER B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy and Interne, 2014. P. 268-295. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163 Acesso em outubro de 2017.

Em tese, as políticas de privacidade conteriam as informações necessárias e suficientes para a tomada de uma decisão racional e ponderada por parte dos cidadãos acerca de consentir ou não com a forma de coleta, uso e cessão de dados. Contudo, quando perguntados sobre as impressões que tinham tido após a leitura das políticas de privacidades dos referidos sites, o resultado foi insatisfatório: 43% respondeu que tinha entendido a maior parte; 21% respondeu que havia entendido completamente; 14% não entendeu a maior parte do que tinha lido; 12% não estava seguro se tinha entendido ou não; 6% não sabia responder ou não se lembrava; e, por fim, 4% não tinha entendido nada das políticas de privacidade.

Quando perguntados sobre o motivo de não lerem as políticas de privacidade, 55,7% respondeu que não lia por serem documentos muito extensos ou muito difíceis de entender (8,7%).7,4% dos usuários responderam que não ligavam para as políticas de privacidade, ao passo que 6,8% dos entrevistados achavam que independentemente de sua leitura, os sites certamente iriam ignorar suas próprias políticas de privacidade no tratamento dos dados colhidos. Outros indicaram que não tinham conhecimento acerca de políticas de privacidade, não sabiam onde encontrá-las ou não tinham nada a esconder. Esse resultado aponta que, apesar de os cidadãos terem o direito à privacidade como um direito de estimado valor, atribuíam pouca importância ao exercício de seus direitos, mostrando pouco interesse na leitura das políticas de privacidade[175].

Além desse problema, ainda existe a assimetria na distribuição de poder. Aqueles que coletam e processam dados possuem muito mais conhecimento técnico do que a média dos usuários. Laura Schertel aponta para o risco dessa assimetria nas relações de consumo: "o consumidor, por ser o polo vulnerável da relação, possui grande dificuldade de controlar o fluxo de dados e de informações pessoais no mercado, bem como de adotar medidas de autoproteção contra os riscos desse processamento"[176].

Apesar de os modelos baseados no consentimento e na autodeterminação informacional terem muitas virtudes, eles nem sempre refletem como as pessoas usam a Internet e as mídias sociais, por exemplo. Ao navegar na internet, existem vários pedidos de consentimento que tomariam boa parte do tempo dos usuários. Dado esse grande número de pedidos de consentimento, os usuários geralmente não consideram realmente as questões

[175] CUSTERS B.H.M., HOF S. van der; SCHERMER B. (2014). Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy and Interne, 2014. P. 268-295. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163 Acesso em outubro de 2017.
[176] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.23.

formuladas por aqueles responsáveis pelos tratamentos de dados, e não parecem avaliar de fato as consequências do consentimento. Ao que conclui Custers[177], os usuários parecem simplesmente consentir quando são confrontados com um pedido de consentimento, o que é obviamente problemático, tendo em vista que isso demonstra a perda de significado do consentimento.

Essa perda do próprio significado do consentimento pode ser sintetizada pela expressão "mito do consentimento". Argumenta-se que esse procedimento aparenta ser inócuo e ilusório[178], dado que os seus efeitos não demonstram contornos muito nítidos ao interessado, quer seja por informações insuficientes ou falta de transparência. Sobre essa falta de controle e consentimento ilusório, Rodotà argumenta:

> (...) é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejo de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente poderá sair como perdedor.[179]

Como resultado desse mito do controle, os usuários parecem cada vez menos engajados no processo de consentimento, clicando de maneira cega nas "caixas de consentimento" quando elas se parecem com outras caixas de diálogo. As pessoas indicam que estão preocupadas com a sua privacidade, mas ao mesmo tempo divulgam informações pessoais por conveniência, descontos e outros incentivos, ou mesmo por falta de entendimento das consequências decorrentes dessa divulgação[180].

Não bastassem esses motivos, Doneda aponta ainda que a impessoalidade que impera nas relações comerciais, e principalmente nas realizadas o*nline,* é outro fator que induz

---

[177] CUSTERS B.H.M., HOF S. van der, SCHERMER B.W., APPLEBY-ARNOLD S., BROCKDORFF & N. Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, Scripted: A Journal of Law and Technology, 2013. P. 435-457. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134 Acesso em outubro de 2017.

[178] EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. Duke Law & Technology Review, Forthcoming,2017. Disponível em: SSRN: https://ssrn.com/abstract=2972855. Acesso em novembro de 2017.

[179] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 77.

[180] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.

a uma "falsa segurança na revelação de informações de caráter pessoal e, consequentemente, no consentimento para seu tratamento"[181].

O exemplo utilizado para demonstrar essa imparcialidade é o "fenômeno do estranho". É comum que pessoas estranhas recebam atenção e lhes sejam confiadas revelações sobre assuntos muito pessoais, que dificilmente – quando não jamais – seriam reveladas a pessoas conhecidas ou mesmo íntimas. Isso seria justificado pela certeza de que a revelação feita não implicará em um julgamento e suas possíveis consequências por parte de um estranho. Essa mesma lógica é muitas vezes aplicada à atividade de fornecer informações pessoais a sites na internet, por exemplo, tratando-se de uma manifestação tecnológica do fenômeno do estranho.

Combinado com o modelo de negócio que prevalece na Internet hoje, o chamado *zero-price advertisement business*[182], em que o consumidor não paga uma quantia monetária para acessar e utilizar serviços e produtos, o fenômeno do estranho pode levar à vulnerabilidade do usuário. Isto porque diante dessa imparcialidade ilusória e dada à falta de informações e transparência, o indivíduo pode não estar ciente do valor de seus dados e dos riscos aos quais está submetido. Ele pode não ter conhecimento de como seus dados pessoais estão sendo rentabilizados, minerados e comercializados para a entrega de publicidade comportamental ou conteúdo direcionado, por exemplo. Como comenta Rodotà,

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações.[183].

A falta de engajamento no processo de consentimento por parte dos usuários pode indicar também, segundo Custers[184], que os usuários geralmente sentem que não têm controle quando lidam com decisões acerca de consentimento, principalmente por causa da lógica do *"take it or leave it":* no caso da recusa em consentir, o acesso a um site ou a um serviço na internet é negado ou severamente prejudicado. Sobre essa problemática que Bruno Bioni chama

---

[181] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 374.

[182] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[183] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 77.

[184] CUSTERS B.H.M., HOF S. van der, SCHERMER B.W., APPLEBY-ARNOLD S., BROCKDORFF & N. Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law, Scripted: A Journal of Law and Technology, 2013. P. 435-457. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134 Acesso em outubro de 2017.

de "lógica binária do *take it or leave it"*[185], Donilo Doneda questiona a própria liberdade da escolha do usuário ao ser confrontado com uma decisão que implica um ônus tão grande na fruição do produto ou serviço oferecido:

> O confronto com situações reais revela que, em tais situações, a pessoa que opta por exercer seu poder de autodeterminação e não revelar seus dados pessoais, no mais das vezes se vê alijado do acesso a determinados bens ou serviços – para cuja fruição o fornecimento dos dados era um passo essencial. A disparidade de meios entre a pessoa, de quem são exigidos os dados pessoais, e aquele que os solicita faz com que a verdadeira "opção" seja tantas vezes a de "tudo ou nada", "pegar ou largar"[186].

Ainda sobre as consequências do não consentimento, Custers aponta para um aspecto importante: com o constante desenvolvimento do Big Data e o aumento de sua capacidade de previsão, há ainda a possibilidade de previsão de informações até mesmo das pessoas que não consentiram, com base nas informações daqueles que consentiram. Nesse caso, mesmo quando a previsão não é precisa, há o risco de se chegar a conclusões equivocadas e, consequentemente, decisões que afetarão negativamente esses usuários, levando a uma possível discriminação[187]. Assim, mesmo o negar do consentimento não garante que a privacidade o usuário esteja protegida.

Laura Schertel, citando Mayer-Schönberger, questiona: "será que nós alcançamos o estágio ótimo da proteção de dados se garantirmos os direitos à privacidade que, quando exercidos, acarretarão a exclusão do indivíduo da sociedade?"[188] Diante do atual sufocamento do controle dos dados pessoais pela lógica binária do *take it or leave it*[189], parece ser o caso.

Entretanto, um dos maiores problemas hoje no cenário da avaliação da eficácia do consentimento tem em sua raiz a própria estrutura de funcionamento do Big Data. Apesar da dificuldade exposta de engajamento dos usuários com o processo de consentimento, esse problema pode ser muito mais profundo, ligado à própria estruturação dos regulamentos sobre proteção de dados. Um problema que coloca de um lado a inovação tecnológica e do outro as garantias dos cidadãos na tutela de seus dados pessoais.

---

[185] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[186] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 373.

[187] CUSTERS, Bart. Click here to consent forever: Expiry dates for informed consent. Big Data & Society, 2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 . Acesso em outubro de 2017.

[188]MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Phiip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The Mit Press, 2001. Apud MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p.61.

[189] BIONI, Bruno. Op. Cit. p. 28.

Tal problema consiste na dificuldade em se limitar o uso de dados a finalidades determinadas sendo que um dos próprios objetivos da tecnologia do Big Data é alargar esse uso dos dados pessoais. Cada vez mais são descobertas novas possibilidades, novos cruzamentos de dados e a uma grande velocidade. Sendo assim, por mais que o pedido de consentimento específico, inequívoco e para cada etapa do tratamento de dados, seja importante para a autodeterminação informacional, aos poucos ele vai se tornando incompatível, obsoleto, uma vez que o constante progresso do Big Data aumenta de forma exponencial os usos que se podem fazer de uma mesma base de dados[190].

Como constata o relatório produzido pelo Instituto de Tecnologia & Sociedade do Rio de Janeiro em 2016[191], a regulamentação da proteção de dados enfrenta uma crise em alguns de seus elementos mais centrais e tradicionais, e o livre consentimento individual é um deles. Tal assertiva apenas corrobora o que o próprio Rodotà já havia percebido: é impossível fundar a proteção da privacidade apenas no consentimento[192]. Esse mecanismo, que um dia foi o eixo central da proteção de dados, está pouco a pouco passando para uma posição complementar à medida que cada vez mais dados pessoais não estão sendo coletados diretamente dos indivíduos ou estão sendo coletados sem o seu conhecimento.

O relatório indica que o Big Data, juntamente com as inovações relacionadas com a Internet das Coisas (Internet of Things – IoT), continuará a mudar o cenário referente aos dados pessoais, o que exigirá uma adaptação da disciplina de proteção de dados pessoais a essas novas circunstâncias, seja adequando as ferramentas e os princípios existentes, seja criando novos meios para a aplicação de leis.

Tal desafio remete a uma investigação de como as novas legislações propostas estão lidando com essas dificuldades relacionadas ao consentimento.

[190] Ibidem, p. 48.

[191] Big data no projeto Sul Global. Relatório sobre estudos de caso. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em: <http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big_-Data_PT-BR_v2.pdf>. Acesso em: outubro de 2017.

[192] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008, p. 77

CAPÍTULO 3: ANÁLISE DO CONSENTIMENTO NO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU E NO PROJETO DE LEI 5.276/2016

Após terem sido tratados vários pontos teóricos acerca do consentimento, neste capítulo será feita uma análise de como duas normativas recentes acerca da proteção de dados pessoais tratam o consentimento. A abordagem será dividida em 3 partes. Na primeira, será feita uma investigação de como alguns pontos do consentimento são tratados no Regulamento Geral de Proteção de Dados (RGPD) europeu. Na segunda, com base nos mesmos critérios, a mesma investigação será feita tendo como objeto o Projeto de Lei brasileiro 5.276/16. E por fim, será feita uma comparação entre esses pontos de ambos os documentos.

Como as normativas são extensas e o consentimento relaciona-se a várias etapas do tratamento de dados, a análise de cada documento será limitada a quatro pontos, com base nas premissas teóricas que já foram levantadas no capítulo anterior. O primeiro ponto a ser analisado é o de (1) como as duas legislações trataram da adjetivação do consentimento na sua definição. Em seguida, (2) se há alguma previsão de revogação do consentimento em seus dispositivos. E por fim, dadas as dificuldades atuais apontadas no capítulo 2 envolvendo o consentimento, serão buscadas duas alternativas nesses documentos: (3) se as legislações preveem alguma alternativa à lógica "*take it or leave it*"; e (4) se as legislações oferecem alternativas para o consentimento, visto que a tendência na doutrina tem sido a perda de sua centralidade na proteção de dados pessoais.

3.1 O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD) EUROPEU

3.1.1. O MODELO EUROPEU DE PROTEÇÃO DE DADOS PESSOAIS

Dos conjuntos de soluções adotadas para a disciplina da proteção de dados pessoais, pode ser feito um agrupamento em dois modelos que sintetizam uma determinada abordagem do problema: o modelo americano e o europeu. De acordo com a doutrina, existe a tendência à uma polarização entre eles e à convergência das legislações a um destes modelos[193].

Enquanto União de Direito, a União Europeia, composta por seus 28 Estados-Membros[194], possui uma construção jurídica própria, tendo as ordens jurídicas nacionais sido transformadas em ordens jurídicas parciais. Da mesma forma que o Estado cria direito e

[193] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 222.
[194] Informação disponível em: https://europa.eu/european-union/about-eu/countries_pt. Acesso em novembro de 2017.

vincula-se a ele, assim o faz a União Europeia, criando seu próprio direito e vinculando-se a ele, com instituições próprias, processos para emitir e interpretar normas, bem como e mecanismos de sanção – estando o poder público da EU submetido a esse direito[195].

Em decorrência da criação desse direito europeu, as Constituições nacionais e as ordens jurídicas que dela derivam perderam a primazia de outrora e passaram a ser Constituições dos Estados-Membros da EU, cujos conteúdos tiveram que ser adaptados à construção europeia[196].

No que diz respeito à disciplina da proteção de dados, o modelo europeu estrutura-se em torno de uma Diretiva, "uma disciplina ampla e detalhada que é transposta para a legislação interna de cada estado-membro"[197]. Segundo Doneda, a Diretiva é um instrumento normativo típico da EU, constituindo uma fonte secundária no sistema de fontes do direito comunitário e com a função básica de uniformização legislativa.

Com a aprovação de uma Diretiva, cada país-membro tem um certo período de tempo para adaptar seu próprio ordenamento jurídico aos novos moldes estabelecidos, num processo que ganha o nome de transposição. Nesse processo, a falha de um país-membro a transpô-la tempestivamente acarreta um certo grau de eficácia direta da diretiva e também leva o país a responder pela mora perante a Corte Europeia de Justiça[198].

Um dos objetivos dessa adaptação é não apenas a redução dos atritos entre os vários ordenamentos, mas também promoção de valores pelos quais a UE pretende orientar-se[199]. Um desses valores é a proteção aos direitos fundamentais, sendo a referência máxima a Carta dos Direitos Fundamentais da União Europeia (CDFUE), que adquiriu força juridicamente vinculante desde o Tratado de Lisboa, em vigor desde 2009[200]. Dentre os direitos fundamentais elencados, está a proteção aos dados pessoais, como pode ser visto em seu art. 8º:

> Artigo 8º - Proteção de dados pessoais
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de consentir com os dados coletados que lhes digam respeito e de obter a respectiva retificação.

[195] SILVEIRA, Alessandra. Princípios de Direito da União Europeia. Doutrina e Jurisprudência. Coleção Erasmus – Ensaios e monografias – Linha de Direito e Ciências Políticas. 2ª edição atualizada e ampliada. Lisboa: Quid Juris – Sociedade Editora, 2011.P. 26-38.
[196] Ibidem, p. 27.
[197] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 222.
[198] Ibidem, p. 224.
[199] Ibidem, p. 225.
[200] SILVEIRA, Alessandra. Op. Cit., p. 71.

> 3. O cumprimento destas regras fica sujeito à fiscalização por parte de uma autoridade independente.

Interessante apontar que essa proteção aos direitos fundamentais é levada a sério a ponto de se permitir que os particulares possam invocar suas disposições diretamente junto aos tribunais nacionais, como forma de fazer valer seus direitos fundamentais protegidos pela ordem jurídica europeia. Existem critérios para que a disposição europeia goze de efeito direto, como a clareza e a incondicionalidade da disposição. Mas ao longo do tempo, esses quesitos têm sido flexibilizados pelo Tribunal de Justiça da União Europeia (TJUE), como afirma Alessandra Silveira[201].

Em precedente de 2005, o TJUE decidiu que "os particulares têm o direito de invocar disposições europeias que não gozam de efeito direto, com vista a obter uma interpretação conforme do direito interno por parte do juiz nacional". De acordo com Alessandra Silveira , o TJUE "tem reduzido gradativamente a fronteira entre a possibilidade de invocar o princípio da interpretação conforme e a possibilidade de invocar uma diretiva com o intuito de excluir a aplicação do direito nacional contrário ao Direito da União"[202].

Segundo a jurisprudência assente do TJUE, as diretivas não gozam de efeito direto horizontal, ou seja, não criam, por si mesmas, obrigações para os particulares – têm como destinatários apenas os Estados-Membros. Mas muitos direitos fundamentais contemplados pela CDFUE gozam de efeito direto horizontal e são concretizados sob a forma de diretivas[203].

O direito à proteção de dados, por exemplo, é concretizado na Diretiva 95/46/EC, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais singulares e à livre circulação desses dados. Essa Diretiva foi promulgada em outubro de 1995 e representava o padrão mínimo de proteção em toda a área da UE.

Ela estabelecia uma terminologia básica em seu art. 2º, prática comum às leis relacionadas com tecnologia. Depois, apresentava princípios que vinculam a coleta, o tratamento e a utilização de dados. Princípios para observação pelos estados-membros em suas legislações internas., e não direitos com suas correlatas garantias e deveres[204].

---

[201] SILVEIRA, Alessandra. Princípios de Direito da União Europeia. Doutrina e Jurisprudência. Coleção Erasmus – Ensaios e monografias – Linha de Direito e Ciências Políticas. 2ª edição atualizada e ampliada. Lisboa: Quid Juris – Sociedade Editora, 2011.P. 73.
[202] Ibidem, p. 75.
[203] Ibidem, p. 73-74.
[204] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. P. 238.

Ocorre quem em 27 de abril de 2016, foi aprovado o novo Regulamento (UE) 2016/679, o Regulamento Geral de Proteção de Dados ou GDPR (*General Data Protection Regulation*) relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O regulamento revogou a Diretiva 95/46/CE (o antigo Regulamento Geral sobre a Proteção de Dados), mas manteve seus objetivos e princípios[205] a saber:

> (3) (...) harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros

O novo regulamento trouxe inovações, que passam a valer a partir de 25 de maio de 2018[206]. Mas para o presente trabalho, o enfoque será apenas no que esse novo documento traz sobre o consentimento na proteção de dados pessoais, especificamente no que diz respeito a alguns critérios.

3.1.2. O consentimento no RGPD

(1) A ADJETIVAÇÃO DO CONSENTIMENTO

O novo Regulamento Geral de Proteção de Dados assim adjetiva o consentimento no item 32 das considerações e no item 11 de seu art. 4º:

> (32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. (...) O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.
> Art. 4º
> 11) «Consentimento» do titular dos dados: uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

Como pode ser visto, são utilizados os adjetivos "livre", "específica", "informada" e "inequívoca". Além disso, o consentimento deve "abranger todas as atividades de tratamento

[205](9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos (...)". Considerando nº 9 do Novo Regulamento. Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679 Acesso em outubro de 2017.
[206] Disponível em: http://www.internetlab.org.br/pt/tags-semanario/uniaoeuropeia/ Acesso em agosto de 2017.

realizadas com a mesma finalidade". Ao mencionar "todas as atividades", a remissão pode ser ao adjetivo "específico". Mas ao mesmo tempo, "finalidade determinada" e "todos esses fins" aponta para o outro adjetivo da "finalidade determinada". De acordo com a abordagem escalável apresentada por Bruno Bioni no capítulo 2, a carga de participação do titular dos dados poderia ser classificada como máxima, como se verá a seguir.

O regulamento dá muita importância ao consentimento informado (item 42; art. 13,1). É importante que o titular conheça a identidade do responsável pelo tratamento e as finalidades a que ele se destina, bem como o destinatário dos dados pessoais. Dessa forma o usuário poderá emitir uma manifestação de vontade com "conhecimento de causa", o que reforça a ideia da autodeterminação informativa. As informações devem ser prestadas de forma concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, recorrendo à visualização sempre que for adequado (item 58).

O titular deve ser informado da definição dos perfis e das consequências que daí advêm, bem como da obrigatoriedade de fornecer seus dados pessoais e das consequências de não os facultar (item 60). Sempre que o responsável pelo tratamento tiver a intenção de tratar os dados para outro fim para o qual não tenham sido recolhidos inicialmente, ele deve fornecer informações aos usuários (item 61).

O consentimento verdadeiramente livre é igualmente exigido. Se o consentimento não for fruto de uma escolha verdadeira ou livre, ou se o titular não puder recusar nem retirar seu consentimento sem ser prejudicado, então ele não é válido por não ter sido concedido de maneira livre (item 43, art. 7º , 4).

É importante também que o titular seja devidamente informado da operação de tratamento de dados e de suas finalidades, que devem ser colocadas de modo transparente, de modo que o usuário tenha uma perspectiva geral do tratamento previsto (item 60, item 63). Aqui se incluem conhecimento da identidade dos destinatários dos dados pessoais e, quando tiver por base a criação de perfis, das suas consequências (item 63).

O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos deverá ser autorizado apenas se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Para se averiguar a compatibilidade da nova finalidade com a inicial, para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento deve demonstrar a existência de uma ligação entre a primeira e a segunda finalidade. As expectativas dos usuários que consentiram também devem ser levadas em consideração (item 50).

(2) POSSIBILIDADE DE REVOGAÇÃO DO CONSENTIMENTO

Mesmo que o usuário tenha consentido, é possível que ele tenha o direito a que seus dados sejam apagados, no caso de direito ao esquecimento ou necessidade de retificação. Um exemplo é se o titular tiver dado o seu consentimento quando criança e ainda não totalmente ciente dos riscos inerentes ao tratamento. Seria possível a supressão desses dados pessoais, mesmo que mais tarde (item 65).

De acordo com o ponto 3 do art. 7º, o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, devendo ser informado dessa possibilidade antes mesmo de dar seu consentimento. A retirada não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. De acordo com o dispositivo, o consentimento deve ser tão fácil de retirar quanto de dar.

(3) POSSIBILIDADE DE ALTERNATIVA À LÓGICA "*TAKE IT OR LEAVE IT*"

Tendo em vista que o consentimento baseado nessa lógica binária não permite que o titular de dados tenha qualquer tipo de escolha ao recusar parte de um tipo de tratamento, por exemplo, uma das alternativas seria o direito de oposição a fases do processamento e compartilhamento de dados.

No art. 21, item 2, o regulamento assim estipula:

> Art. 21 – Direito à oposição
> 2. os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
> 3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.

O dispositivo permite que o usuário tenha um poder de escolha sobre a formação de perfis e sobre o compartilhamento de dados com os terceiros. Seria uma forma, portanto, de o cidadão exercer uma autorização fragmentada no que diz respeito ao fluxo de dados pessoais, uma autorização voluntária. Nesse sentido, o consentimento seria feito de uma maneira mais livre, uma vez que o cidadão não estaria sendo obrigado ao compartilhamento de seus dados com terceiros, por exemplo, para poder ter acesso a um produto ou serviço.

(4) POSSIBILIDADE DE OUTROS MODOS DE LEGITIMAR O TRATAMENTO DE DADOS PESSOAIS

No item (40), o consentimento é visto como apenas uma das formas para legitimar o tratamento de dados pessoais:

> "(40) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar".

No caso, são apresentados outros "fundamentos legítimos". No caso, outras formas que legitimam a licitude no tratamento são apresentadas no art. 6º:

> Art. 6ºLicitude do tratamento
> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O consentimento é apenas uma das formas de se verificar a licitude. Aparece também a opção de "interesses legítimos" na alínea "f". O tratamento é lícito se ele "for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros". A consideração 47 discorre um pouco mais sobre o que seria esse interesse legítimo:

> 47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber

> se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.

De acordo com o dispositivo, o interesse legítimo pode ser um fundamento jurídico para o tratamento de dados pessoais, tomando em conta as expectativas razoáveis dos titulares dos dados e desde que não prevaleçam os interesses ou liberdades individuais do usuário. Uma das situações em que pode haver um interesse legítimo é quando existir uma relação "relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento".

Consoante o item 50, o tratamento de dados pessoais para outros fins deve ser autorizado somente se for compatível com as finalidades para os quais os dados pessoais tenham sido coletados inicialmente:

> (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. (...)O fundamento jurídico previsto no direito da União ou dos Estados-Membros para o tratamento dos dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior. A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas

No caso dessa mesma finalidade para tratamentos diversos, não seria necessário um fundamento jurídico diverso. É requerida uma avaliação para saber se o titular de dados pode prever de maneira razoável, no contexto da coleta, que seus dados podem ser tratados com essa

finalidade diferente embasada no interesse legítimo. Uma aplicação prática seria a utilização de dados para a prevenção e controle de fraude. O usuário não seria obrigado a consentir sobre esse tipo de tratamento, estando ele fundado em um interesse legítimo àquele que controla os dados, alinhado aos interesses do cidadão e que não violando sua privacidade.

3.2. O PROJETO DE LEI 5276/16

3.2.1. O MODELO BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS E O CONTEXTO DO PROJETO DE LEI

Diferentemente do modelo europeu, o modelo brasileiro ainda não conta com uma lei geral de proteção de dados, um único instrumento legal com a previsão de normas gerais, princípios, direitos e procedimentos. Diante da ausência dessa lei geral no país, o que é feita é uma harmonização das mais diversas normas sobre proteção de dados que protejam a personalidade do cidadão, com a utilização do próprio Código Civil, o Código de Defesa do Consumidor, a lei do cadastro positivo e a lei de acesso à informação pública, dentre outras[207].

Em defesa à proteção da intimidade, como explicitada no art. 5º, X da Constituição Federal, o Marco Civil da Internet foi uma das leis a regular esse tema. Após intensa participação social por meio de consultas públicas em plataformas digitais e muito debate público[208], foi editada a Lei 12.695/14, mais conhecida como Marco Civil da Internet.

Baseado na neutralidade, liberdade de expressão e privacidade, o Marco Civil estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Ele tem como princípios, como expressos em seu art. 3º, II e III, a proteção da privacidade e a proteção dos dados pessoais – esta, na forma de lei. Nesse caso, seu objetivo principal não é regular de maneira detalhada a proteção aos dados pessoais. O Marco Civil deixa a tarefa a cargo de uma lei específica ulterior.

Boa parte dos direitos assegurados ao usuário estão contidos no art. 7º do dispositivo, tais como a inviolabilidade da intimidade e da vida privada e sua proteção (inciso I), e o não fornecimento a terceiros de seus dados pessoais, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (inciso VII). Além disso, o cidadão tem

[207] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 141.
[208] Disponível em: >http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-ptbr.pdf> Acesso em novembro de 2017.

direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, por exemplo (inciso VIII).

Entretanto, como já foi exposto, essa lei não aborda todas as especificidades necessárias para a regulamentação da proteção de dados pessoais. Nesse sentido, em fevereiro de 2015, o Ministério da Justiça retomou a pauta de 5 anos anteriores de um anteprojeto de lei sobre proteção de dados pessoais[209]. Por meio de uma plataforma no site Pensando Direito[210], foi aberta uma consulta pública para receber contribuições de toda a sociedade. A plataforma ficou disponível por 10 meses, até julho de 2015, e recebeu mais de 2.000 contribuições do setor empresarial, da comunidade científica e acadêmica, sociedade civil e dos próprios cidadãos de forma individual. Em maio de 2016, com poucas modificações, o anteprojeto foi transformado no Projeto de Lei nº 5.276/2016[211], que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

De acordo com o relatório "Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil", o projeto de lei tramitava em caráter de urgência constitucional, com uma espécie de pressão para que o rito de aprovação ocorra de forma mais abreviada e célere. Ao invés de 10 sessões legislativas e uma tramitação progressivas nas comissões, o projeto

> Ao invés 10 (dez) sessões legislativas e uma tramitação progressiva nas Comissões designadas para a sua apreciação , o PLPDP/EXE deverá ser analisado em 05 sessões e de forma simultânea por todas elas. Essa economia procedimental deve resultar, necessariamente, na sua análise em até 45 (dias) a contar da data do seu recebimento na Câmara, sob pena do trancamento da pauta da casa[212].

Em 6 de julho de 2016, entretanto, o presidente interino Michel Temer retirou o projeto do regime de urgência. Na semana seguinte, por proposta do deputado Alexandre Leite (DEM-SP), o PL 5276/2016 foi apensado ao PL 4060/2012, o que contribuiu para reestabelecer a indefinição a respeito de sua aprovação[213]. Naquele mesmo ano, foi assinada uma carta aberta

---

[209] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 28. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[210] A plataforma pode ser acessada em: http://pensando.mj.gov.br/dadospessoais/ Acesso em agosto de 2017.

[211] Disponível em: http://pensando.mj.gov.br/dadospessoais/2015/04/ministerio-da-justica-prorroga-debate-sobre-protecao-de-dados-pessoais/. Acesso em agosto de 2017.

[212] BIONI, Bruno. Op. cit, p. 5.

[213] Disponível em: http://www.internetlab.org.br/pt/semana-especial-protecao-de-dados-pessoais/ Acesso em novembro de 2017.

de apoio ao PL 5276/16 pelas principais entidades de defesa de direitos digitais no Brasil, como GPoPAI/USP, Coding Rights, Intervozes, Idec, Proteste, MediaLab, ITS/Rio, CTS/FGV, Lavits e inclusive o LAPIN, grupo de pesquisa em Direito Privado e Internet da Universidade de Brasília[214].

Como o próprio relatório "Xeque-mate" aponta, além do PL 5276/2016 de autoria do Poder Executivo, existem outras iniciativas legislativas em andamento que dizem respeito à proteção de dados pessoais. São elas o Projeto de Lei do Senado Federal nº 330/2013 – combinado com o 181/2014 e 131/04 – e o Projeto de Lei da Câmara dos Deputados, o 4060/2012. Todos esses projetos visam regulamentar de maneira ampla a proteção dos dados pessoais no Brasil.

Contudo, o PL 5276/2016 tem sido visto como o mais relevante por ter sido melhor construído, de forma mais democrática, e o que está mais apto a proteger a privacidade dos cidadãos no que diz respeito à tutela de dados pessoais. Por tais motivos foi escolhido o PL 5276/2016 para a análise do presente trabalho. Segundo a carta aberta, as entidades destacam que o texto "foi construído de forma colaborativa com amplo engajamento social por meio de duas consultas públicas"[215] , reforçando a extensa duração de debate público e o considerável número de contribuições dos diversos ramos da sociedade civil, acadêmica e empresarial[216].

E essas contribuições de fato tiveram repercussões. O documento afirma que "as diferenças e modificações entre as versões pré e pós-consulta pública do texto do anteprojeto são claros indicadores de que se procurou chegar a uma redação equilibrada a salvaguardar a inovação e a proteção da privacidade dos cidadãos"[217]. Em 2017, durante o 8º Seminário de Proteção à Privacidade e Dados Pessoais realizado em São Paulo pelo Comitê Gestor da Internet no Brasil, a Coalizão Direitos na Rede[218] realizou o lançamento da campanha "Seus dados são você", com o objetivo de sensibilizar a população e o Parlamento "sobre a urgência da aprovação de uma Lei de Proteção de Dados Pessoais no Brasil, tendo em vista os atuais modelos de negócio e a atuação dos poderes públicos baseados na coleta massiva de dados"[219].

[214] Disponível em: https://www.codingrights.org/pt/pl-de-dados/. Acesso em novembro de 2017.
[215] Ibidem.
[216] Ibidem.
[217] Ibidem.
[218] "Uma rede independente de organizações da sociedade civil, ativistas e acadêmicos em defesa da Internet livre e aberta no Brasil" .Disponível em: https://direitosnarede.org.br/c/seus-dados-sao-vc/. Acesso em novembro de 2017.
[219] Disponível em: https://direitosnarede.org.br/blog/. Acesso em novembro de 2017.

Atualmente, o PL 6291/2016 encontra-se apensado ao PL 5276/2016, que por sua vez encontra-se apensado ao PL 4060/2012. Como última ação legislativa[220] está a designação de uma Comissão Especial para proferir parecer. E segundo a Agência da Câmara, a comissão especial ainda estava na fase de audiência pública em julho de 2017[221].

Dado esse contexto da proteção de dados pessoais no Brasil e de uma das principais iniciativas legislativas do país sobre a temática, será dado prosseguimento à investigação proposta no trabalho, a saber a análise de determinados critérios acerca do consentimento no PL 5276/2016.

3.2.2. O CONSENTIMENTO NO PL 5276/16

(1) A ADJETIVAÇÃO DO CONSENTIMENTO

Antes da própria definição de consentimento no PL, cabe notar que a autodeterminação informativa é um dos primeiros fundamentos dispostos no art. 2º. Considera-se consentimento a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", conforme o art. 5º, VII. O art. 7º fala que o tratamento de dados pessoais somente poderá ser realizado "mediante o fornecimento pelo titular do consentimento livre, informado e inequívoco". De acordo com a classificação escalável elaborada por Bruno Bioni, a carga de participação nesse PL é intermediária, por não fazer menção a um consentimento expresso e específico[222].

Sobre o consentimento informado, o art. 8º é claro ao exigir que o titular tenha "acesso facilitado às informações sobre o tratamento de dados". Essas informações devem ser disponibilizadas de forma clara, adequada e ostensiva sobre a finalidade específica do tratamento, sobre, entre outros:

> Art. 8º
> 1 – finalidade específica do tratamento;
> II – forma e duração do tratamento;
> III – identificação do responsável;
> IV – informações de contato do responsável;

---

[220] Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em novembro de 2017.

[221] Disponível em: http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/537765-COMISSAO-ESPECIAL-SOBRE-TRATAMENTO-DE-DADOS-PESSOAIS-TEM-AUDIENCIA-NESTA-TARDE.html Acesso em novembro de 2017.

[222] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 46. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

> V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados e o âmbito de sua difusão;
> VI – reponsabilidades dos agentes que realizarão o tratamento; e
> VII – direitos do titular, com menção explícita à possibilidade de:
> a) acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado
> b) denunciar ao órgão competente o descumprimento de disposições desta Lei; e
> c) não fornecer o consentimento, na hipótese em que o consentimento é requerido mediante o fornecimento de informações sobre as consequências da negativa

Ademais, nos parágrafos seguintes do art. 8º, são dispostas outras facetas do consentimento. Na hipótese em que o consentimento é requerido, ele será considerado nulo "caso as informações fornecidas ao titular tenham conteúdo enganoso ou não tenham sido apresentadas previamente de forma clara, adequada e ostensiva", conforme §1º. É vedado, de acordo com o art. 9º §4º o tratamento de dados pessoais quando o consentimento tenha sido obtido "mediante erro, dolo, coação, estado de perigo ou simulação".

Em caso de alterações na identificação, o titular deverá ser informado (art. 8º §2º), bem como periodicamente caso as atividades que importem coleta de dados pessoais sejam continuadas (art. 8º§3º), Nesse caso, ele deverá ser informado de forma periódica sobre as principais características do tratamento.

(2) POSSIBILIDADE DE REVOGAÇÃO DO CONSENTIMENTO

Consoante disposição do art. 9º §5º, "o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular". Aqui cabe um acréscimo: o §6º prevê a possibilidade de renovação do consentimento, em caso de alteração de informação na finalidade específica, forma e duração do tratamento, e na identificação do responsável e respectivos contatos.

(3) POSSIBILIDADE DE ALTERNATIVA À LÓGICA "*TAKE IT OR LEAVE IT*"

Nos termos do art. 8º §4º, quando o consentimento para o tratamento de dados for "condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados".

Tal disposição caracteriza o que Bruno Bioni denomina "consentimento granular"[223], uma forma de limite à economia dos dados pessoais e também de fortalecimento

[223] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 55. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

do consentir enquanto uma manifestação de vontade livre. Dessa forma, o usuário tem disponível a seu favor "meios pelos quais poderá exercer controle sobre o tratamento de seus dados", não ficando preso à possibilidade de exclusão parcial ou completa de um produto ou serviço, e podendo exercer melhor seu direito à autodeterminação informativa.

(4) POSSIBILIDADE DE OUTROS MODOS DE LEGITIMAR O TRATAMENTO DE DADOS PESSOAIS

No art. 9º, §7, o PL prevê que o órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que ele é fornecido e a natureza dos dados pessoais que estão sendo fornecidos. Tal disposição já demonstra uma possibilidade de flexibilização do consentimento, uma das formas de legitimação do tratamento de dados.

No art. 7º, na seção sobre os requisitos para o tratamento de dados, estão listadas várias outras formas de legitimar o tratamento de dados pessoais, sendo o consentimento apenas uma delas:

> Seção I – Requisitos para o tratamento
> Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco;
> II – para o cumprimento de uma obrigação legal pelo responsável
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;
> IV – para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais/
> V – quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular de dados;
> VI – para o exercício regular de direitos em processo judicial ou administrativo/
> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII – para a tutela de saúde, com procedimento realizado por profissionais da área da saúde ou por entidade sanitárias;
> IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevaleceram interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

O tratamento de dados pode ser realizado com base em 9 hipóteses, sendo o consentimento apenas uma delas. De acordo com o art. 10º, o legítimo interesse do responsável "somente poderá fundamentar um tratamento de dados pessoais quando necessário e baseado em uma situação concreta, respeitados os direitos e liberdades fundamentais do titular".

O §1º art. 10 apresenta que esse interesse legítimo deve comtemplar as expectativas do titular quanto ao tratamento de dados. O §2º aponta para a necessidade de adoção de

medidas que garantam a transparência do tratamento nessa hipótese, como o fornecimento aos titulares de mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

O §3º estabelece que nessa forma de tratamento de dados baseada no interesse legítimo, "somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento". E o §4º possibilita ao órgão competente solicitar ao responsável um "relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo"

O art. 6º apresenta que, de acordo com o princípio da finalidade, o tratamento deve ser realizado para "finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades".

3.3. ANÁLISE COMPARADA: ASSIMETRIAS E SIMILITUDES

(1) A ADJETIVAÇÃO DO CONSENTIMENTO

Pela análise da extensão dos adjetivos atrelados ao consentimento, foi percebido que no Regulamento Geral de Proteção de Dados europeu a carga de participação do titular de dados é maior, tendo em vista a menção ao adjetivo "específico". Nessa escala, o consentimento é relativo a um escopo de consequências muito mais detalhadas. O regulamento utiliza também o adjetivo "explícito", diferentemente do PL.

Já no PL 5276/16, a carga de participação seria intermediária, por não conter o adjetivo "específico" ou "expresso". Mas importante notar que o próprio Marco Civil já exige que o consentimento seja expresso, conforme art. 7º, VII.

Em ambas as legislações, o consentimento deve ser uma manifestação de vontade livre, informada e inequívoca/explícita. A informação é frisada em ambos os documentos, devendo ser disponibilizada de forma acessível, clara, adequada e de fácil compreensão. Apesar de o PL afirmar a importância da autodeterminação informativa como um fundamento da disciplina de proteção de dados, o Regulamento é bem mais enfático no papel da informação para que o usuário emita uma manifestação de vontade com "conhecimento de causa", expressão utilizada pelo próprio documento.

Mas ao mesmo tempo, o PL frisa causas de nulidade do consentimento, e uma delas é o caso de informações de conteúdo enganoso ou que não tenham sido apresentadas de forma

prévia, clara, adequada e ostensiva. Isso o assemelha ao Regulamento também na exigência de um consentimento verdadeiramente livre.

Em ambas normativas, o titular deve ser informado, dentre outros aspectos, sobre a identidade do responsável pelo tratamento de dados e sobre o destinatário. E todas as informações devem ter acesso facilitado. Também se faz presente a necessidade de informar o cidadão das consequências de sua negativa no consentimento de dados. Sempre que essa finalidade mude, o usuário deve ser informado.

Apesar de elencar uma série de tipos de informações que devem ser facilitadas ao usuário, o PL não faz menção específica à transparência na formação de perfis como o faz o Regulamento, que pode ser um bom instrumento contra as discriminações decorrentes da mineração de dados, criação e classificação de perfis, técnicas abordadas no capítulo 1 deste trabalho.

A finalidade do tratamento também é mencionada, devendo ser sempre informada e seguida por aquele que trata os dados. Caso seja alterada, também deve haver notificação ao cidadão. Um ponto em que o Regulamento se destaca é na exigência de uma ligação entre a primeira e a segunda finalidade, como forma de se avaliar a compatibilidade da nova finalidade com a inicial.

(2) POSSIBILIDADE DE REVOGAÇÃO DO CONSENTIMENTO

Acerca da possibilidade de revogação, ambos os documentos preveem o direito de deixar de consentir, que pode ser exercido a qualquer momento. O Regulamento ainda cita exemplos e dispõe que "o consentimento deve ser tão fácil de retirar quanto de dar". Importante perceber que em nenhum dos casos, é apresentada a necessidade de justificativa, o que nesse ponto se assemelha ao caso alemão apresentado no capítulo 2 por Laura Schertel.

De acordo com as premissas do capítulo anterior sobre a importância de se possibilitar a revogação do consentimento, ambos os documentos absorvem esse direito de "mudar de ideia", inerente ao próprio direito da personalidade. E como foi visto, dogmaticamente falando, a possibilidade de revogação do consentimento sem justificativa parece ser a mais adequada.

(3) POSSIBILIDADE DE ALTERNATIVA À LÓGICA "TAKE IT OR LEAVE IT"

Esse foi um ponto com abordagens bem diferentes entre os dois documentos. No Regulamento UE, existe a possibilidade de se opor à uma etapa do processo de tratamento de dados, como a comercialização. Essa foi identificada como uma forma de o titular exercer uma autorização fragmentada, voluntária, quanto ao fluxo de dados pessoais, o que seria uma alternativa à lógica do *take it or leave it* envolvendo o usufruir de serviços ou produtos.

É questionável, entretanto, o momento dessa oposição e se de fato ela seria uma alternativa de "consentimento granular"[224], como denomina Bruno Bioni. É certo que o usuário seria informado da possibilidade do direito de oposição no momento de consentir. Mas tecnicamente, essa hipótese não parece ser sobre a escolha, no momento do consentimento, de aspectos a se consentir. O usuário consente com tudo e sabe que depois poderá se opor a alguma forma de tratamento. O momento desse consentimento granular também não fica muito explícito no PL ao dispor que o usuário será informado dos "meios pelos quais poderá exercer controle sobre o tratamento de seus dados".

Caso a capacidade de controle dos dados por parte do cidadão seja transferida apenas para depois do início do tratamento desses dados, sua carga de participação pode ser marginalizada[225], assemelhando-se à sistemática do *opt-out*. Como se o usuário devesse manifestar apenas o seu interesse em sair – no caso, de se opor – uma vez que o pressuposto seria o de concordância máxima. Mas o sistema que parece melhor captar a essência da autodeterminação informativa é o *opt-in*[226], em que o usuário deve consentir de forma inequívoca quanto ao tratamento de seus dados pessoais. E nesse sentido, a situação mais semelhante à essa sistemática seria a que possibilitasse ao usuário escolher, no momento do consentimento, quais e como seriam fornecidos seus dados pessoais.

O ideal para o consentimento granular seria se o cidadão, no momento do consentimento, pudesse escolher, por exemplo, quais os tipos de dados pessoais que seriam coletados (se geolocacionais, contatos telefônicos e etc.), quais os tipos de tratamento de seus dados (se para fins de entrega de conteúdo direcionado, fins de publicidade comportamental e etc.), o quanto tempo e frequência do tratamento de seus dados, bem como se haveria ou não o compartilhamento dos dados com terceiros[227].

---

[224] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 54. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.
[225] Ibidem, p. 46.
[226] Ibidem, p. 46.
[227] Ibidem, p. 54.

A hipótese identificada no Regulamento parece coadunar com essa quarta possibilidade de escolha do cidadão, enquanto a do PL não é muito específica na forma desse "exercício de controle" proposto. De qualquer forma, são dispositivos que apontam um caminho que limita a economia de rede sustentada pelos dados pessoais, como exposto no capítulo 1. Esse tipo de consentimento granular seria uma forma conferir ao usuário um "poder de barganha"[228], à medida em que ele poderá escolher a forma como seus dados serão tratados – no mínimo no que diz respeito ao compartilhamento de seus dados - e usufruir dos serviços/produtos oferecidos. Seria uma alternativa que contrabalancearia a necessidade exigida por quem demanda os dados e que efetivaria uma manifestação de vontade do usuário de forma muito mais autônoma e livre[229].

(4) POSSIBILIDADE DE OUTROS MODOS LEGÍTIMOS PARA O TRATAMENTO DE DADOS PESSOAIS

Foi interessante notar que ambos os documentos trazem o consentimento como apenas uma das formas de legitimar o tratamento de dados. Enquanto o Regulamento UE prevê outras 6 possibilidades, o Projeto de Lei prevê ainda 8 hipóteses. E dentro dessas hipóteses, será abordada a dos "interesses legítimos".

Para o Regulamento UE, o consentimento não deixa de ser importante. Mas ele reconhece casos específicos em que outras questões – que não o consentimento - justificariam a licitude do tratamento de dados. Seria uma forma de flexibilização da sistemática baseada apenas no consentir. No Brasil, o PL prevê que o órgão competente adeque os requisitos do consentimento, considerando o contexto e a natureza dos dados, o que caracterizaria também uma flexibilização do consentimento. Isso aliado às outras 8 hipóteses para autorizar a coleta, uso e tratamento de dados.

Como foi inicialmente abordado no capítulo 2, uma das dificuldades de um consentimento específico está na própria estrutura do Big Data, tecnologia que tem como objetivo o próprio alargamento do uso de dados pessoais. Por mais importante que seja para a autodeterminação o pedido de consentimento específico, inequívoco, e para cada etapa do tratamento de dados, aos poucos ele vai se tornando incompatível e obsoleto, uma vez que o

[228] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 46. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.
[229] Ibidem, p. 46.

constante progresso do Big Data aumenta de forma exponencial os usos que podem ser feitos de uma mesma base de dados.

Por isso uma abordagem normativa mais flexível faz-se necessária, "com previsões legais para o tratamento adicional dos dados pessoais sem qualquer tipo de consentimento posterior do titular"[230]. E uma dessas formas é a exceção à regra do consentimento, método adotado tanto na Diretiva da União Europeia quanto no PL.

O Regulamento já prevê, por exemplo, o retratamento de dados pessoais. E nesse caso, não seria necessário perguntar de novo ao usuário se ele consente ou não com essa nova forma de tratamento. Como o documento expõe, o tratamento de dados para outros fins que não aqueles para os quais os dados tenham sido coletados inicialmente não precisa de fundamento jurídico distinto daquele que permitiu a coleta de dados iniciais. Contanto que haja uma ligação entre a primeira e a segunda finalidade. Essa, inclusive, seria uma forma de se permitir a continuidade do progresso tecnológico sem abandonar a proteção dos dados pessoais dos cidadãos.

A ligação também está relacionada à previsibilidade – se o usuário já poderia esperar, no momento do consentimento, um tratamento adicional de seus dados. A expressão utilizada pelo Regulamento UE é se o usuário já poderia "razoavelmente prever" esse segundo tratamento a ser abarcado pelo interesse legítimo.

Essa forma de interesses legítimos abordada no novo Regulamento Europeu parece ser uma regulamentação de vanguarda[231] , quem sabe até inaugurando uma nova geração de proteção de dados, no sentido de abraçar as rápidas e constantes evoluções tecnológicas do Big Data, mas ao mesmo tempo sem abrir mão da garantia da proteção de dados pertencente aos cidadãos.

O PL 5.276/16 parece seguir o mesmo caminho traçado pelo sistema jurídico europeu de proteção de dados. Dentre as hipóteses que autorizam o tratamento de dados pessoais, o PL inclui os interesses legítimos do responsável ou de terceiros. Como apontam Laura Schertel e Danilo Doneda ao analisar o projeto de lei, a hipótese é relevante "ao

[230] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 48. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[231] GOMES, Rodrigo Dias de Pinho. Desafios à privacidade: Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf>. Acesso em setembro de 2017.

reconhecer que outras partes – além do próprio titular – podem ter interesses protegidos juridicamente no processamento, uso ou circulação de determinadas informações"[232].

Na perspectiva de Bruno Bioni, a terminologia "legítimos interesses" é equívoca, uma vez que dá margem a várias interpretações enganosas. O autor assim explica:

> A terminologia legítimos interesses é equívoca, o que permitiria uma série de interpretações se estas fossem realizadas de forma assistemática das demais disposições da diretiva e, sobretudo, frente à regra geral do consentimento. Ou seja, tal hipótese não se dá no vácuo, mas dentro da dinâmica de regra geral em que há uma relação pré-estabelecida na qual o titular consentiu para um uso específico ou para uma finalidade determinada de seus dados (...)[233]

Fora da sistemática elaborada pelo PL, a impressão que se tem da hipótese do legítimo interesse é de uma brecha na lei, de uma possibilidade muito ampla e elástica a ponto de abarcar qualquer interesse que os detentores do tratamento de dados pessoais aleguem. Nesse sentido, é bastante preocupante porque, de pronto, já parece que a hipótese por sua natureza ameaça a proteção dos usuários.

A impressão é de que as empresas detentoras de dados alegariam como legítimos quaisquer interesses para colocar em risco a privacidade dos usuários. Parece até mesmo que quem elaborou a lei esqueceu-se da proteção de dados nesse quesito. Entretanto, não é o caso – e esse é o ponto de Bruno Bioni. Essa cláusula não deve ser lida como uma "válvula de escape geral, a partir da qual qualquer tratamento de dados pessoais passa a ser autorizada"[234]. Apesar de exigir sim limites, a hipótese do "legítimo interesse" deve ser analisada dentro do contexto normativo do PL, como será demonstrado a seguir.

Inicialmente, o usuário consente em fornecer seus dados a uma empresa, por exemplo, para uma finalidade determinada. O que ocorre na situação da demanda pelo legítimo interesse é que quem coletou os dados pessoais demanda utilizá-los novamente para outra finalidade, agora nova, mas muito próxima daquela original. Diante disso, surge a questão: se o usuário já consentiu para a finalidade x, ele haveria de consentir de novo para uma finalidade tão próxima a x? Parece não ser necessário.

É nesse sentido que surge a importante possibilidade dos interesses legítimos no PL, assim como aparece no novo Regulamento UE, ainda mais num contexto de Big Data em

---

[232] MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. Revista de Direito Civil Contemporâneo, vol. 9/2016. P. 35-48. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/107466. Acesso em agosto de 2017.

[233] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 48. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.

[234] MENDES, Laura Schertel; DONEDA, Danilo. Op. cit, p 35-48.

que a utilização secundária ocorre quase que corriqueiramente. E nessa utilização secundária, muitas vezes a finalidade é muito próxima da finalidade da utilização inicial, por assim dizer.

Assim, quem coletou os dados demanda utilizá-los novamente, de modo a ser alcançado pela hipótese do interesse legítimo sem que haja um consentimento posterior do titular. A própria autorização anterior do usuário e o fato de a nova finalidade ser próxima à finalidade anterior autorizariam o novo tratamento sem um novo consentimento do titular.

Claro que a legitimidade dessa demanda deve ser verificada de acordo com a compatibilidade entre esse novo uso, o uso adicional, e aquele que originou a coleta de dados pessoais[235]. Como foi dito, essa exceção ao consentimento, a hipótese dos interesses legítimos, não se dá no vazio, mas "na conjuntura de que houve um consentimento prévio que parametriza o novo uso (adicional) dos dados pessoais"[236]. O propósito secundário e o original devem ser próximos um do outro, demandando uma análise do contexto para verificar se esse uso está de acordo com as legítimas expectativas do titular dos dados pessoais[237].

E como foi visto, o PL, da mesma forma que o Regulamento UE, apresenta parâmetros claros "para que a exceção dos interesses legítimos tome um lugar restrito na dinâmica normativa da proteção de dados pessoais"[238]. Caso contrário, a regra geral do consentimento tornaria-se uma exceção, tamanha a elasticidade e as diversas facetas que a "hipótese camaleão dos interesses legítimos"[239] poderia alcançar.

Esses parâmetros foram abordados na seção anterior e dizem respeito a mecanismos de transparência sobre os novos tratamentos de dados e necessidade de compatibilidade das novas finalidades. Um dos requisitos é que o legítimo interesse seja baseado em uma situação concreta, devendo ser respeitados os direitos e liberdades do titular de dados, e que as expectativas do titular devem ser levadas em consideração.

Outro parâmetro é a minimização dos riscos à privacidade, como por meio da anonimização dos dados. E por fim, a possiblidade de o órgão competente fiscalizador solicitar um relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo, como uma forma de auditar essas "práticas de mercado".

---

[235] BIONI, Bruno. Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil, p. 49. Disponível em; http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf Acesso em agosto de 2017.
[236] Ibidem, p. 49.
[237] Ibidem, p. 49.
[238] Ibidem, p. 49.
[239] Ibidem, p. 49.

CONSIDERAÇÕES FINAIS

O presente trabalho procurou analisar inicialmente como as transformações tecnológicas levaram a uma nova configuração econômica e social, de forma que hoje ela é pautada na informação. Diante de um cenário em que os dados possuem valor econômico e o imperativo dos novos negócios da vigilância visa a captação dos dados pessoais, o consentimento foi abordado como a forma pelo qual o usuário mantém-se informado e pode autorizar ou não a coleta, processamento e compartilhamento de seus dados pessoais na rede.

O papel do consentimento dentro do contexto da proteção de dados pessoais foi desenvolvido à luz da autodeterminação informativa e como um instrumento de legitimação do tratamento de dados. Para tanto, foram abordados seus pressupostos de validade, sua natureza jurídica e possibilidade de revogação. O trabalho também apresentou as recentes críticas ao consentimento, bem como suas dificuldades e desafios. Por fim, fez-se uma análise comparada sobre como o Regulamento Geral de Proteção de Dados (RGPD) e o Projeto de Lei brasileiro 5276/16 sobre proteção de dados pessoais abordam a temática do consentimento.

A análise foi feita com base em quatro pontos, a saber: como as legislações tratam da adjetivação do consentimento, se há previsão de revogação do consentimento, se as legislações preveem alguma alternativa à lógica do *take ir or leave it*, problema demonstrado no capítulo 2, e se, diante da recente perda de centralidade do consentimento, haveria nesses documentos outras alternativas para além do consentimento que permitissem o controle como forma de tutela de dados pessoais.

Da comparação, foi possível observar que apesar da diferença de carga participativa nos dois documentos - possuindo o consentimento no Regulamento carga maior do que o consentimento no PL - a adjetivação ainda é muito parecida, sendo o consentimento em ambas as legislações definido como manifestação de vontade livre, informada, inequívoca, explícita. Ambos prezam pela necessidade de informação adequada, acessível, clara, para que o titular de dados tome decisões bem ponderadas e conscientes.

Mas como foi visto, apenas uma mudança em como as informações são transmitidas para o cidadão não é suficiente para uma possível reversão da crise do consentimento, visto que um dos maiores problemas está relacionado ainda à própria insuficiência do modelo baseado no consentimento face às constantes evoluções do Big Data.

Sobre a possibilidade de revogação do consentimento, ambos os documentos parecem ter absorvido da doutrina a importância dessa hipótese como inerente ao próprio exercício do direito da personalidade. Ainda mais quando essa hipótese não precisa ser justificada, o que a doutrina entende ser a mais adequada na proteção dos dados pessoais.

A despeito da possibilidade de alternativa à lógica do *take ir or leave it,* foram encontradas formas de o usuário se opor a certa etapa do tratamento de dados, como a comercialização no caso do Regulamento UE. Entretanto, seria uma oposição pós-consentimento por parte do titular dos dados, e não de fato uma escolha no próprio momento do consentimento, como seria o ideal. Já o PL menciona "outros meios" pelos quais o usuário poderá exercer o controle de seus dados, mas não há um maior detalhamento para identificar o momento do exercício desse controle.

Nesse ponto conclui-se que talvez ainda haja dificuldades de previsão e implementação de um consentimento granular ou fragmentado. Seria uma forma de aumentar o "poder de barganha" do titular dos dados pessoais frente à sempre alegada necessidade de coleta de dados para a fruição de um serviço ou produto.

Sobre a possibilidade de outros modos para legitimar o tratamento de dados pessoais, foi interessante notar que ambos os documentos trazem o consentimento como apenas uma das formas de legitimar o tratamento de dados. No Regulamento UE o consentimento não deixa de ser importante, mas ele parece não ser tão mais central como antes. O mesmo acontece com o PL, mas de maneira mais tímida.

Tanto no Regulamento como no PL há a possibilidade de interesses legítimos, o que também é bastante positivo para a legislação brasileira, que parece seguir os passos de uma forma promissora europeia de se entender o consentimento. Nessa hipótese de interesse legítimo, quem coletou os dados pessoais demanda utilizá-los novamente para outra finalidade, agora nova, mas muito próxima da finalidade original. Sendo assim, haveria a necessidade do titular consentir novamente? Ao que tudo indica não. Caso haja uma ligação entre essas duas finalidades, seria uma hipótese de novo tratamento de dados legítimo e sem o pedido de consentimento.

Claramente essa é uma hipótese que retira a centralidade do consentimento, ainda mais em um contexto de Big Data, em que a todo momento são descobertas novas formas de cruzamento de dados. Se o consentir com cada uma dessas finalidades parecidas de tratamento (como na utilização secundária) for importante para proteger a personalidade do titular de dados, por outro ele parece criar um volume enorme de pedidos de consentimento

para o cidadão. E como já se viu, isso não garante necessariamente sua proteção. Com essa avalanche de pedidos de consentimento, por assim dizer, este poderia continuar sendo um instrumento inequívoco.

Ao contrário, a hipótese de interesse legítimo, apesar de não pedir mais o consentimento toda vez, como estamos acostumados, seria uma forma de conciliar as rápidas e constantes evoluções tecnológicas do Big Data sem abrir mão da garantia da proteção de dados atinente aos cidadãos. Isso talvez pudesse ser o traçar de uma solução para o "problema estrutural" do consentimento, em que ele seria obsoleto por tentar determinar todas as finalidades específicas para o uso de dados em pleno auge do Big Data com a utilização secundária de dados. Além de diminuir a sobrecarga de informações aos cidadãos.

E como já foi demonstrado, longe de constituir uma brecha ou uma possibilidade muito ampla ou elástica. Pelo contrário, uma hipótese com freios e contrapesos.

Por fim, conclui-se que o PL 5276/16, na maior parte dos itens elaborados e à sua maneira, segue o mesmo caminho traçado pelo sistema jurídico europeu, o que pode ser considerado positivo, visto a atualidade do Regulamento Geral de Proteção de Dados da UE e sua preocupação com a proteção de dados. Seria como se o PL já nascesse atualizado e espelhado em um modelo compromissado com a garantia da privacidade e tutela de dados pessoais.

Mas por enquanto, ainda é necessário que se aprove no país uma lei geral sobre o tema, para que de fato possamos falar em um regime jurídico brasileiro de proteção de dados pessoais suficientemente detalhado.

REFERÊNCIAS BILBIOGRÁFICAS

BENKLER, Yochai. *The wealth of networks: how social production transforms markets and freedom.* In: New Haven and London: Yale University Press, 2006. Disponível em: <http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf>.

BIONI, Bruno. *Xeque-mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil*. Disponível em; <http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf>

BOYD, Danah; CRAWFORD, Kate. *Critical questions for big data. Provocations for a cultural, technological, and scholarly phenomenon.* Information, Communication & Society. Vol. 15, 2012. Disponível em: <http://dx.doi.org/10.1080/1369118X.2012.678878

CASTELLS, M.; CARDOSO, G. *A Sociedade em Rede: Do Conhecimento à Ação Política.* Belém: Imprensa Nacional – Casa da Moeda, 2005. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/a_sociedade_em_rede_do_conhecimento_a_acao_politica.pdf>.

CRAWFORD, Kate; SCHULTZ, Jason. *Big data and Due Process: Toward a Framework to Redress Predictive Privacy Harms.* In: Boston College Law Review, vol. 55, 2014. Disponível em: <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>.

CUSTERS B.H.M., HOF S. van der, SCHERMER B.W., APPLEBY-ARNOLD S., BROCKDORFF & N. *Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law*, Scripted: A Journal of Law and Technology, 2013. P. 435-457. Disponível em:< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134>

CUSTERS B.H.M., HOF S. van der; SCHERMER B. *Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy and Internet*, 2014. P. 268-295. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163>

CUSTERS, Bart. *Click here to consent forever: Expiry dates for informed consent.* Big Data & Society,2016. DOI: 10.1177/205395171562493. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047128 .

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

DONEDA, Danilo; SCHERTEL MENDES, Laura. *Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016*. Revista de Direito Civil Contemporâneo, vol. 9, p.35-48, out-dez 2016.

EDWARDS, Lilian; VEALE, Michael. *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For.* Duke Law & Technology Review, Forthcoming,2017. Disponível em: <https://ssrn.com/abstract=2972855>.

ENISA, *Privacy by Design in Big Data*. Disponível em: <https://www.enisa.europa.eu/publications/big- data-protection>.

GOMES, Rodrigo Dias de Pinho. *Desafios à privacidade: Big Data, consentimento, legítimos interesses e novas formas de legitimar o tratamento de dados pessoais*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/03/Rodrigo-Gomes.doc-B.pdf>.

GONÇALVES, Andrey F. L., BERTOTTI, Monique e MUNIZ, Veyzon C. *O direito fundamental à privacidade e à intimidade no cenário brasileiro na perspectiva de um direito à proteção de dados pessoais.* In: Doutrinas Essenciais do Direito Constitucional. Revista dos Tribunais. Vol. 08/2015, p. 597-614.

INTERNETLAB. *O que está em jogo no Anteprojeto de Lei de Proteção de Dados Pessoais?* Disponível em: < http://www.internetlab.org.br/pt/internetlab-reporta/o-que-esta-em-jogo-no-anteprojeto-de--lei-de-protecao-de-dados-pessoais/>

ITS, *Big data no projeto Sul Global. Relatório sobre estudos de caso*. Instituto de Tecnologia & Sociedade do Rio. Rio de Janeiro, 2016. Disponível em:<http://itsrio.org/wp-content/uploads/2016/03/ITS_Relatorio_Big -Data_PT-BR_v2.pdf>.

MCDONALD, A.M.; CRANOR LF. *The cost of reading privacy policies*. I/S Journal for Law and Policy for the Information Society. Privacy Year in Review, 2008. Disponível em: <http://www.aleecia.com/authors-drafts/ reading. PolicyCost-AV.pdf.>.

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

RAMIRO, Livia F. M., DE LUCCA, Newton. *A tutela da privacidade e a proteção à identidade pessoal no espaço virtual*. In: Direito, Governança e novas tecnologias – V Encontro Internacional do Conpedi Mentevidéu – Uruguai. Coordenadores: Marcelo Eduardo Buza Reilly, Roseane Leal da Silva. Florianópilis: CONPEDI, 2016. Disponível em:< https://www.conpedi.org.br/publicacoes/9105o6b2/v4u5j0t6/lZL7VI9LojzjW2o3.pdf>

RODOTÀ, Stefano. *A vida na sociedade da vigilância – a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda – Rio de Janeiro: Renovar, 2008.

SCHERMER, B. W.; CUSTERS, Bart; HOF. S, van der. *The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection*. Ethics and Information Technology, 2014. DOI: 10.1007/s10676-014-9343-8. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418>.

SILVEIRA, Alessandra. *Princípios de Direito da União Europeia. Doutrina e Jurisprudência*. Coleção Erasmus – Ensaios e monografias – Linha de Direito e Ciências Políticas. 2ª edição atualizada e ampliada. Lisboa: Quid Juris – Sociedade Editora, 2011.

SOLOVE, DJ (2013) *Privacy self-management and the consent dilemma*. Harvard Law Review 126: 1880–1903. Disponível em:<https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/>.

WARREN, Samuel; BRANDEIS, Louis. *The Right to Privacy*, In: Harvard Law Review, Vol. 4, No. 5, 1890. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf >.