XII EPCC ENCONTRO INTERNACIONAL DE PRODUÇÃO CIENTÍFICA DA UNICESUMAR 19 a 21 de outubro de 2021
ISSN 2594-4991
ISBN 978-65-5615-456-5

A POSSIBILIDADE DE ALIENAÇÃO DE DADOS PESSOAIS E A NOVA LEI GERAL DE PROTEÇÃO DE DADOS

Javan Eduardo Ribeiro de Castro[1]

[1] Acadêmico do Curso de Direito, Campus Maringá/PR, Universidade Estadual de Maringá (UEM). javaneduardo@gmail.com

RESUMO

Esta pesquisa tem como problemática central averiguar a possibilidade de alienação de dados, amparado pelo consentimento do titular, no contexto da nova Lei Geral de Proteção de Dados. Como forma de concretização disso, foi utilizado o método dedutivo com revisão de obras bibliográficas doutrinárias, posições jurisprudenciais e demais produções científicas sobre o tema, além de sucintos casos fáticos. Dado contexto, foi realizado um estudo acerca das posições doutrinárias sobre o direito à privacidade, concomitante com uma retrospectiva histórica sobre esse. Assim, adotou-se a abordagem de Sarlet *et al*. acerca das delimitações, ou falta delas, de privacidade para fundamentar as discussões propostas. Adiante, são examinados os conceitos apresentados pela Lei 13.709/18, em seu art. 5º, destacando aqueles que fundamentam a relação jurídica discutida na problemática. Conseguinte, realiza-se uma breve análise sobre a concepção de consentimento no direito privado brasileiro, levantando hipóteses sobre os limites de sua validade. Por fim, leva-se à baila o debate da permissibilidade do texto legal a respeito da alienação de banco de dados em casos fáticos, conjugando-os com os obstáculos latentes ostentados pelas balizas do consentimento do usuário.

PALAVRAS-CHAVE: Consentimento do titular; Direito à privacidade; Tecnologia.

1 INTRODUÇÃO

A massiva produção de dados no cotidiano e o surgimento de tecnologias capazes de analisá-los e dar finalidades econômicas em larga escala, como técnicas de engenharia de dados, é motivo de dúvida e preocupação, essa justificada por juristas e demais profissionais que não estão habituados com a marcha acelerada da tecnologia.

Com objetivo de proteger os titulares de dados de possíveis abusos praticados por empresas responsáveis pelo tratamento deles, a Lei Geral de Proteção de Dados (LGPD) veio com a difícil missão de concretizar um objetivo tão abstrato e mutável como a *garantia da privacidade*.

Nesse contexto, aliado com os enevoados horizontes apresentado pela Lei 13.709/18, resta uma premente necessidade de análise sobre a legalidade de transações de dados. Isto fica ainda mais evidente pela ausência latente de trabalhos acadêmicos e doutrinários sobre a problemática, dado o pequeno lapso de tempo da publicação da lei, urgindo-se por uma análise detalhada.

Assim, este trabalho busca, através de uma extensa leitura e estudo de obras bibliográficas doutrinárias, artigos científicos e legislação vigente, responder à seguinte problemática central: diante a nova LGPD, seria possível o estabelecimento de um mercado legal de alienação de dados?

Como forma de sanar tal pergunta, o primeiro capítulo se dedica a delimitar o conceito de privacidade, peça fundamental a qual a LGPD busca resguardar, valendo-se de concepções doutrinárias diversas, apresentando uma corrente majoritária e partidária da definição mais fechada e sólida, e outra minoritária, que admite uma maior maleabilidade do conceito. Além disso, é concedido uma breve retrospectiva histórica do surgimento e desenvolvimento do direito à privacidade.

Adiante, no segundo capítulo, faz-se um exame da conceituação dos termos apresentados no rol do art. 5° da lei de dados brasileira, investigando seus possíveis desdobramentos em casos concretos, realizando breves comparações com a legislação europeia, e, tecendo comentários e críticas às escolhas normativas.

ISSN 2594-4991
ISBN 978-65-5615-456-5

Já no terceiro capítulo, avalia-se o pivô da relação jurídica discutida, o consentimento, demonstrando as eventualidades de invalidez desse, bem como os grandes desafios ostentados para que não seja esvaziado a concordância dos usuários, principalmente em uma conjuntura de contratos de adesão e as dificuldades do homem médio em relação à tecnologia.

Neste cenário, ainda no último capítulo, delibera-se sobre as hipóteses de alienação de dados, com e sem o consentimento do titular, bem como será sobrepesado o aceite em relação aos obstáculos do consentimento, como forma de solucionar os litígios em situações fáticas.

2 LEI GERAL DE PROTEÇÃO DE DADOS E SEUS CONCEITOS

A Lei Geral de Proteção de Dados (LGPD) trouxe uma conceituação muito mais explícita em relação aos termos que utiliza no decorrer do texto normativo. Parte disso se deve ao fato da Constituição Federal (BRASIL, 1988) ter baixa densidade normativa, ao passo que uma lei ordinária se espera um alto grau, principalmente ao regulamentar temas específicos. Em seu art. 5° (BRASIL, 2018), a LGPD faz referência a 19 definições, de densidade normativa variada, que são os alicerces para o resto da legislação se fundamenta, como forma de entender a possibilidade de alienação de dados pessoais, é imprescindível que haja uma compreensão concreta sobre as ferramentas que a LGPD dispõe.

O primeiro conceito apresentado é o de dado pessoal, sendo definido normativamente como *informação relacionada a pessoa natural identificada ou identificáve*l (BRASIL, 2018). Válido citar, que expressões como “identificada” e “identificável” não são exclusividade da LGPD. Estas se apresentam, também, em outras leis, como, por exemplo, na Lei 12.527/2011 - Lei de Acesso à informação, em seu art. 3°, IV[1] (BRASIL, 2011), para a definição de informação pessoal, que ao refere-se, ambos, ao mesmo conceito.

Em questão normativa, a redação do artigo foi orientada quase que estritamente em razão da formulação dada pela *General Data Protection Regulation - GDPR*[2] (EUROPA, 2016) -, ato legislativo europeu, o qual descreve em seu art. 4°, §1, como *qualquer informação relacionada a uma pessoa natural identificada ou identificável* (tradução nossa)[3]” (2018).

Como Bioni aponta (2016, p. 18 e 21), há duas correntes para a definição de dados pessoais, reducionista e expansionista. Porém, faz a ressalva que “ambas demandam uma análise contextual de onde está inserido um dado, aferindo-se o seu grau de identificabilidade” (p. 18). Logo, faz-se a seguinte distinção:

> A orientação reducionista baseia-se em uma lógica restritiva pela qual dado pessoal é uma informação que deve estar associada a uma pessoa específica. Ele deve ser um signo que permita estabelecer de forma imediata ou direta um vínculo com o seu titular, individualizando-o de forma precisa [...]. Enquanto que a expansionista aposta em uma lógica mais flexível, que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta. Um dado para ser pessoal deve ser, portanto, a projeção de uma pessoa identificável. (BIONI, 2016, p. 17).

[1] IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
[2] Regulamento Geral de Proteção de Dados (tradução nossa).
[3] *any information relating to an identified or identifiable natural person.*

ISSN 2594-4991
ISBN 978-65-5615-456-5

Assim, extrai-se que para tal definição, numa ótica reducionista, os dados têm que fazer referência direta a pessoa para torná-lo um dado pessoal. Ou seja, é necessário que o dado seja capaz de identificar o indivíduo de modo preciso (e.g. em um contexto de banco de dados extenso, um dado - como número da carteira de identidade - é o bastante para individualizar Jorge, ao passo que seu CEP não seria).

Por outro lado, na visão expansionista, um conjunto de dados, mesmo que não diretamente identificáveis, analisado em contexto, seria capaz de separar uma pessoa dos demais, surgindo então uma capacidade identificadora (e.g. no mesmo contexto de banco de dados, há diversos José da Silva, sem a informação de RG, CPF ou outro dado único, porém, a partir da verificação de demais informações colhidas como CEP e idade, gera-se possibilidade de individualizar).

Deste modo, acreditamos que o legislador se posicionou claramente em uma visão expansionista, principalmente sob o ponto de vista de maior abrangência da tutela aos jurisdicionados, o que poderia restar prejudicado diante casos concretos, caso a ótica reducionista fosse adotada.

Na mesma toada, ainda se tem o conceito de dado sensível, uma espécie de dado pessoal que dispõe sobre assuntos como etnia, religião, opinião política, vida sexual, dados genéticos etc (BRASIL, 2018). Apoiando-se nas lições de Rodotá (2008), Frazão *et al.* (2019) justifica que o escopo da proteção dos dados sensíveis são deslocados estritamente da privacidade, ao passo que flui na direção do princípio da proteção da igualdade e da não discriminação (p. 107).

Nesse caso, que a sensibilidade de tais dados é gerada a partir da potencialidade discriminadora contra indivíduos. O fato é agravado quando um banco de dados sensíveis é utilizado sem maior controle por algoritmos capazes de tomar decisões relevantes, como ocorreu no caso COMPAS[4], que foi demonstrado como capaz de gerar resultados desastrosos e de repercussões diretas nas liberdades individuais fundamentais, como a liberdade de locomoção. Logo, é premente a necessidade de uma tutela cuidadosa do assunto.

Para além, a LGPD (2018) identifica a figura de dados anonimizados e o processo de anonimização, ambos correlatos. Os dados anônimos se diferem dos dados pessoais, pois naquele é impossível de se estabelecer ligação com o seu titular e revelar sua identidade, um dado sem rosto ou nome. Esta anonimidade é estabelecida por meio de processos como o de supressão[5], generalização[6], randomização[7] e pseudoanonimização[8] (BIONI, 2019, p. 105).

É relevante mencionar que em nenhum momento do texto normativo é citado de formas explícitas ou é apresentado um rol, exemplificativo ou não, das formas de anonimização, deixando o processo a cargo do responsável pelo tratamento dos dados, que segundo a LGPD (2018), deve-se valer de métodos razoáveis para que o processo seja bem sucedido.

---

[4] Correctional Offender Management Profiling for Alternative Sanctions - Gerenciamento de Corretividade de Infratores para Sanções Alternativas (tradução nossa). Usado por Estados americanos como Nova York, Wisconsin e Florida. O algoritmo era responsável por assistir juízes acerca da probabilidade do réu em reincidir uma vez livre, influenciando na concessão de liberdades provisórias. Foi exposto que o COMPAS tinha maiores probabilidades de assinalar um alto grau de periculosidade a um agente negro do que um agente branco em iguais condições (YONG, 2018).

[5] Supressão de dados identificadores únicos, como número de registro geral, cadastro único ou CPF.

[6] Supressão ou generalização de partes do nome de uma pessoa (e.g. João da Silva dos Santos poderia se tornar João da Silva ou apenas João, mesclando-se com os demais homônimos).

[7] É a substituição de dados irrelevantes para a estatística que se busca formular por outros fictícios, mascarando-se as informações capazes de identificar o indivíduo (RODRIGUES, 2020).

[8] "Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro." (RODRIGUES, 2020).

ISSN 2594-4991
ISBN 978-65-5615-456-5

Entretanto, nos posicionamos com extremo ceticismo diante uma possibilidade ideal de anonimização. Por mais eficiente que sejam os processos utilizados durante o tratamento, diante de tecnologias e técnicas como *Big Data*, os dados podem sofrer processo reverso que ilumine seu titular com determinado esforço e conhecimento de lógica de dados. Tal fato foi principalmente apontado por Narayanan e Shmatikov (2008, p. 14), ambos cientistas da computação que a partir da disponibilização de avaliações "anônimas" pela empresa de *streaming* Netflix foi realizado um cruzamento de dados em relação aqueles públicos e identificados do *website* IMDB (o perfil dos avaliadores no site contém, geralmente, nomes reais e demais dados únicos, como *e-mail* e telefone celular), um dos maiores da internet em relação a *reviews* de filmes e séries, quebrando o sigilo dos avaliadores do serviço de *streaming*. Quando minerado, o algoritmo desenvolvido foi capaz de reverter a anonimização sem maiores dificuldades.

Salienta-se que o estudo foi publicado há mais de uma década e, mesmo com a tecnologia disponível para a época, alcançou resultados surpreendentes. Assim, são no mínimo preocupantes as possibilidades de violação de dados, atualmente e em um futuro próximo, tendo em vista o avanço tecnológico e as projeções para tecnologias ainda melhores em um futuro não distante.

Em outras palavras, o desenvolvimento das tecnologias também aumenta as possibilidades de violação de dados, causando uma crescente nos riscos de violação à privacidade. Logo, é forçoso reconhecer que a completa anonimidade não passa de uma ilusão efêmera, ou nas palavras de Bioni, "um mito" (2018, p. 108).

Adiante, somos apresentados aos agentes das relações jurídicas reguladas nesta lei. Primeiramente, o titular. Presente no inciso V, ele é definido como "pessoa natural a quem se refere os dados objetos de tratamento (BRASIL, 2018)". Ressalta-se que o legislador, nesse momento, optou por garantir a proteção exclusivamente a pessoas físicas, não abrangendo as jurídicas. Magalhães e Divino (2019, p.87) reconhecem que tal proteção não foi garantida, porém criticam a ausência de previsão legal, e expõe a necessidade de flexibilização legislativa para estender a tutela, principalmente em vista de contratos de pessoas jurídicas em que se tratem de transações financeiras envolvendo seus dados e sua imagem.

Entende-se a necessidade de proteção à pessoas jurídicas, porém discorda-se em parte com o argumentação supracitada. Estender, através de flexibilização, o âmbito de proteção é no mínimo perigoso, ao passo que é golpe duro à legalidade. Deste modo, porque vemos como conflitante com o conceito de "dado pessoal" diante a pessoa jurídica, especialmente na modalidade de dado sensível, poderia uma pessoa não física ser titular dessa modalidade de dados? Outrossim, vemos que a GDPR (EUROPA, 2016), inicialmente, não oferece tal proteção, lei a qual o texto normativo foi fortemente inspirado. Deste modo, acredita-se que determinada flexibilização poderia importar na retirada do protagonismo da proteção da pessoa natural, a qual é objeto central de proteção da LGPD (BRASIL, 2018).

A figura do controlador, operador e encarregado também são ativas na relação de tratamento de dados. Tanto o controlador quanto o operador podem ser pessoas naturais ou jurídicas de direito privado ou público, definidas como agentes de tratamento, ao passo que o encarregado seria necessariamente uma pessoa natural (BRASIL, 2018). Assim, o controlador é o responsável direto pelo tratamento de dados do titular (e.g. empresa X de telefonia), podem terceirizar, ou não, esses serviços para outra empresa (e.g. empresa Y especializada em tratamento). Em questão de direito comparado, ambas figuras correspondem ao *controller* e *processor* respectivamente na legislação européia (EUROPA, 2016). Importando o DPO[9] europeu, a legislação brasileira trouxe o encarregado, definindo-

[9] *Data Protector Officer.*

ISSN 2594-4991
ISBN 978-65-5615-456-5

o como “canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dado” (BRASIL, 2018).

Em questão de responsabilidade civil pelos atos, dependerá de caso a caso. Porém, em linhas gerais, o encarregado nunca responderá pelos danos. Quanto ao controlador e operador, ambos responderão diretamente por violações legais, e quando se tratar de responsabilidade solidária, o controlador responderá se estiver envolvido de forma imediata com tratamento e o controlador se violar algum dispositivo legal ou descumprir ordens do controlador (BODIN DE MORAES, p. 3-5). Porém, faz-se a ressalva que a lei é extremamente em grande parte de seu texto normativo e essas questões abordadas poderão ser amplamente mutadas quando aplicadas pelo judiciário.

3 O CONSENTIMENTO E A ALIENAÇÃO DE DADOS

3.1 CONSENTIMENTO E SEUS DESAFIOS

O consentimento é o pivô de toda discussão sobre dados moderna, sendo peça capaz de delimitar a linha da legalidade durante o tratamento. O consentimento segundo a LGPD é definido como *manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada* (BRASIL, 2018). É necessária análise minuciosa do que foi apresentado.

Como manifestação livre, entende-se como aquela que não é contaminada por vícios de consentimento, os quais são descritos no Código Civil (2002), sendo o erro, o dolo e a coação. A presença de qualquer um desses vícios acarreta a anulabilidade do negócio jurídico praticado (VENOSA, 2018, p. 342).

Tem-se como prudente debater brevemente sobre o erro. Ele é considerado uma falsa presunção da realidade pelo agente que emite o consentimento, devendo-se considerar como substancial no caso fático, e que sem ele, o negócio jurídico não seria concretizado (LÔBO, 2017, p. 460-461). A ignorância caminha lado à lado com o erro, equiparando-se para fins jurídicos, sendo aquele a ausência de qualquer conhecimento (VENOSA, 2018, p. 344).

São raras as situações em que o erro e ignorância são aplicados para anulação de negócios jurídicos pelo judiciário, porém acredita-se que esse instituto possa ter maior força diante à LGPD.

Tendo em vista os conceitos aqui antes tratados, os quais parecem ser de uma complexidade ignorada pela maior parte da população, posicionamos no sentido que o direito não pode se encastelar longe da sociedade a qual é aplicado. Definições, como dados, são intimamente ligados a internet na atualidade, e, hoje, cerca um quarto da população sequer tem acesso à internet, e, ainda, dentro desse percentual, nem metade dispõe de computador ou tablet para realizar o acesso, ficando refém das dificuldades enfrentadas pela telefonia móvel (IBGE, 2020).

O homem médio é amplamente utilizado no direito brasileiro para descrever o comportamento padrão esperado do agente diante de situações cotidianas de um meio social. Porém, considerando essa demografia, nos leva a acreditar que ele é, no mínimo, ignorante em relação a dados pessoais e não compreende em sua completude questões envolvendo o uso da internet. Não é razoável requerer que o cidadão, que não tem nem condições técnicas e não dispõe do saber para realizar uma simples troca de e-mails, que ele conceba as implicações de certas modalidades de tratamento de dados.

Conclui-se então que a eficácia da proteção da LGPD está visceralmente ligada com a democratização do acesso às tecnologias, como a internet, e com a educação do uso destas para a população geral. Na ausência dessas medidas, a LGPD pode ter efeito contrário, constituindo um risco aos direitos que ela pretende amparar.

ISSN 2594-4991
ISBN 978-65-5615-456-5

Interessante demonstrar que durante o processo de colhimento de consentimento deverá constar explicitado as finalidades para qual o tratamento se destina (BRASIL, 2018). Aqui, encontra-se outro desafio para o consentimento.

A concordância do usuário para uso de *app*'s ou outros tipos de serviços, no âmbito da internet, costuma-se dar via de *Terms and Conditions* (T&Cs), contrato de adesão, normalmente apresentado antes da utilização do produto. Bradshaw *et al* (2011) analisaram diversos T&Cs proveniente de empresas que fornecem serviços de computação em nuvem sob demanda. Concluíam que os T&Cs eram formulados minuciosamente para dificultar o acesso à justiça do consumidor, muitas vezes dando interpretação *contra legem* em suas cláusulas, ainda fazendo o alerta que tais práticas não se resumiam a iniciativa privada, mas também a entes públicos (Bradshaw *et al*, 2011, p. 222).

Outro ponto preocupante dos T&Cs foi apontado pelo *Forbrukerrådet,* órgão governamental norueguês de defesa dos interesses do consumidor. O órgão se propôs a ler, em sua completude, todos T&Cs dos *app*'s mais comumente instalados em um celular de um norueguês, entre eles, *Facebook*, *Youtube, Whatsapp* e *LinkedIn,* totalizando 33 aplicativos. A leitura ininterrupta tomou mais de 31 horas, levando o *Forbrukerrådet* a classificar os T&C como absurdamente longos e de demasiada complexidade, tornando boas decisões virtualmente impossíveis de serem tomadas baseadas em tais contratos (BBC, 2016).

Interessante citar que o teórico econômico comportamental, Daniel Kahneman, aborda tal matéria. Utilizando a distinção cunhada por Thaler e Sunstein (2008), de Econs (agente racional, ou ainda, o homem econômico, possui preferências e comportamentos consistentes) e Humanos (agente descrito pela psicologia e economia comportamental, nem sempre têm comportamentos consistentes), argumenta que o primeiro leria cada letra miúdas de um T&C, uma vez que seria fruto de sua racionalidade, mas um humano nunca faria isso, deixando espaço para que *uma empresa inescrupulosa que redige contratos que os clientes costumam assinar sem ler possui considerável margem de manobra legal para ocultar informação importante à vista de todos.*(KAHNEMAN, 2012, p. 441). Ainda, ressalta que é uma implicação perniciosa presumir que os humanos não precisem de uma proteção maior além que a informação relevante esteja exposta no T&C's, fazendo menção a uma variação de fonte e uma linguagem menos complexa para uma tentativa de amenizar o problema (KAHNEMAN, 2012, p. 441).

Em um contexto brasileiro, o consentimento provavelmente estaria incluso nesse emaranhado de cláusulas nos T&Cs.

Assim, entende-se que essa concordância dada pelo usuário poderia ser esvaziada se utilizado esses contratos de adesão, o usuário se encontra em estado de hipervulnerabilidade, como afirma Bioni (2018, p.254), exigir uma decisão elaborada sobre o tratamento de seus dados em um contexto de T&C complexos, extensos e construídos com a finalidade de dificultar o entendimento do usuário de seus direitos, em um contrato de adesão, é colocar sobre os ombros do agente ônus excessivo, principalmente pelo o prisma que esse, em via de regra, como explicitado anteriormente, é desprovido de educação digital. Porém, reconhece-se que não foram elaborados métodos de colheita de consentimento que superem totalmente esses desafios apresentados e que sejam de amplo acesso, mas, também, entende-se que esse fato não pode amenizar a responsabilidade dos controladores e operadores.

Assim, há a necessidade de um crivo forte do judiciário em face de cada caso concreto, analisando as suas peculiaridades e de seus agentes envolvidos.

3.2 A POSSIBILIDADE DE ALIENAÇÃO DE DADOS DIANTE À LGPD

ISSN 2594-4991
ISBN 978-65-5615-456-5

Com o surgimento de uma sociedade informacional, os dados, de modo inegável, passaram a ter valor econômico, e o capitalismo encontrou formas de se adaptar a essa nova realidade de predominância da internet (DA SILVEIRA, 2017, n.p.).

O conglomerado *Alphabet Inc.* (Google, Youtube, Drive) teve um lucro anual, em 2019, de $46.075 bilhões, sendo 83.3% deste apenas em propaganda (TREFIS TEAM, 2019). Na mesma linha seguiu a conglomerado *Facebook Inc.* (Facebook, Instagram, WhatsApp), com um lucro, em 2019, de $70,7 bilhões, sendo 98.5% desse valor em anúncios (JOHNSTON, 2020). Tudo isso é possível através da coleta de dados pessoais dos usuários (geolocalização, idade, renda), utilizando-a para refinar o algoritmo responsável por vender anúncios - e também utilizado para refinar outros serviços (GOOGLE, 2020), gerando um perfil[10] mais preciso do daquele e valorizando cada clique na publicidade mostrada. Os dados se transmutaram de simples informações espaçadas sobre os usuários para bens mercadológicos que movimentam as maiores empresas do mercado mundial.

A mercantilização dos dados também gera impasses. Como exemplo, considerando a seguinte situação hipotética: Empresa Y é especializada em tecnologia e dona de grande repositório de dados pessoais. O governo X está interessado em reduzir os altos índices de delitos ocorridos em determinada região. Como forma de concretização disso, X contrata Y, que inclui em seus produtos, além de robusta infraestrutura de vigilância, um farto banco de dados de moradores de tal região e citadinos propensos a frequentar a vizinhança. Assim, permite-se que o governo X, monitore, através de reconhecimento facial e outras tecnologias, movimentações suspeitas. Até que ponto isso seria ético e dentro dos parâmetros legais?

A situação descrita pode parecer fruto de um futuro distante ou saída diretamente de um dos escritos de Orwell (2009) ou Huxley (2014), porém, ela não está longe de realidade. A sociedade da vigilância elaborada por Foucault (2014) e também trabalhado por Rodotà (2008), já é palpável em solo chinês. O partido único dispõe de mais de 626 milhões de câmeras de segurança espalhadas pelo seu território, mostra tendências de aperfeiçoamento à medida que de fomenta e utiliza os serviços de *startups* focadas em desenvolvimento de tecnologia de reconhecimento facial e a coleta desses dados (DUNDLEY, 2020), os sistemas utilizados são de alta performance, conseguindo a façanha de identificar os cidadãos até quando estes estão com os rostos coberto por máscaras (BORAK, 2020).

A situação da privacidade e da relação do governo chinês com essas *startups,* através do intercâmbio de dados, é tão desenvolvida que já está em curso a implementação de um esquema de crédito social, avaliando as atitudes de cada indivíduo, atribuindo pontos a eles, garantindo serviços, benefícios e punições a cada um deles através desse sistema de pontuação (CREEMERS, 2018). Ou seja, o futuro do cidadão, suas relações interpessoais, sua possibilidade de ascensão social e demais fatores que conduzem sua vida vão estar estritamente ligada a esse sistema, desde lugares que ele pode frequentar até a probabilidade de conseguir um financiamento ou adquirir um imóvel em determinada vizinhança. *Nosedive* já extrapola os limiares turvos da ficção (BLACK MIRROR, 2016).

Especificamente no Brasil, antes da publicação da LGPD, a mercantilização de dados já foi questão, mesmo que superficialmente, tratada pela jurisprudência. O caso concreto foi analisado em sede de Apelação Cível pelo Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS) em ação de indenização por danos morais. A demanda ajuizada por Darcila Becker em face da empresa PROCOB S.A., especializada em consultas e proteção de crédito, foi baseada nas alegações que a empresa Apelada estaria mantendo e comercializando os seus dados pessoais, expondo, consequentemente, sua imagem,

[10] Profiling (tradução nossa).

ISSN 2594-4991
ISBN 978-65-5615-456-5

vida privada, honra e intimidade, violando também o art. 43, §2[11], do Código de Defesa do Consumidor (TJRS, 2014).

A demanda foi rejeitada pelo referido tribunal sob as seguintes justificativa: não se verificava ilegalidade na criação de banco de dados de consumidores, visto que se tratava de "arquivo de consumo" e não há vedação para esta prática no ordenamento; as informações mantidas não atingiram grau de dados pessoais sensíveis; e não haveria exposição desses dados à terceiros mal intencionados, ora que o acesso era restrito à empresas e profissionais com cadastro prévio na plataforma (op. cit. 2014).

A comercialização tratada no Acórdão se limita a consultas de banco de dados por terceiros interessados, com finalidade de proteção de crédito. Não há prática de alienação dos bancos de dados cadastrais pela empresa Apelada a outrem, ou seja, os dados são custodiados pelo controlador durante todo processo, o qual garante a segurança daqueles durante a prestação do serviço. Ainda, as informações armazenadas não se configuram como sensíveis, fundamentando que "interessa à proteção do crédito e às relações comerciais, não se tratando de informação que viole a privacidade do indivíduo" (op. cit. 2014). Sendo assim, mesmo diante da falta de consentimento do consumidor integrante do banco, não há arbítrio na prática, ainda estando regulada, hoje, pela própria LGPD quando dispõe que o tratamento poderá se dar "para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente" (BRASIL, 2018).

Porém, qual seria o estado de legalidade da alienação de banco de dados contendo informações sobre diversos indivíduos, com o consentimento destes à luz da LGPD? Esta é uma questão complexa, com várias nuances, não parece ser possível dar uma resposta definitiva, principalmente em face da novidade da legislação. O que nos resta então é fazer breves ponderações e apontamentos.

Primeiro, acreditamos que a doutrina majoritária se guinará no sentido de reconhecer que é vedado a venda de dados sem o devido consentimento expresso. Salvo hipóteses específicas, o consentimento é pivô nessa relação jurídica, como bem explicitado no art. 7°, I[12] (BRASIL, 2018).

Agora, no que tange a alienação conjugada com consentimento prévio, não vemos óbice no texto normativo. Entende-se que o §5° do artigo supracitado[13], trate, de modo aparentemente superficial, essa possibilidade, exigindo a necessidade de um consentimento específico (BRASIL, 2018).

Infelizmente, devido a recente vigência da lei não é possível se aprofundar em extensas análises doutrinárias ou jurisprudenciais sobre o tema. Entretanto, cremos ser prudente fazer breves alertas sobre essa possibilidade.

Como já abordado anteriormente neste artigo, a privacidade é algo mutável (SARLET *et al.*, p.489), de modo que se ressignifica através das inovações tecnológicas que à ameaçam. Ademais, vemos o consentimento como maior obstáculo para uma implementação do comércio regulamentado de banco de dados. A manifestação da vontade livre e inequívoca é fortemente motivada, tanto pela capacidade da pessoa que a emite como pela forma que ela é colhida. Como foi exposto e fundamentado, o homem médio é

[11] § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
[12] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
[13] § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

ISSN 2594-4991
ISBN 978-65-5615-456-5

ignorante no tocante à privacidade, dados pessoais e seus desdobramentos, ao passo que os métodos de colheita de consentimento (T&Cs), no âmbito da internet, principalmente, são desenvolvidos minuciosamente para gerar empecilho e confusão ao usuário. Deste modo, adota-se a posição que não superar os desafios aqui apontados é esvaziar, de forma completa, qualquer possibilidade de autonomia entre as partes que o consentimento possa conceder. Aplicar *pacta sunt servanda* numa relação jurídica na qual uma das partes é manifestamente hipossuficiente, quando esta não está envolta no erro ou ignorância, ainda agravado pelo contrato de adesão, é algo desmedido e vai de encontro a tudo que a LGPD se propõe, qual seja, a garantia de que o usuário se sinta invulnerado no tratamento de seus dados.

4 CONCLUSÃO

Averígua-se que o direito à privacidade foi resultado de um contexto histórico tipicamente burguês associado com as inovações tecnológicas da época, essas que tinham intimidade com a ampliação do escopo de proteção desse direito, ao passo que demonstravam mais capazes de violá-lo, requerendo uma solução por parte dos ordenamentos. Induz-se também que com o aumento do fluxo de dados produzidos pelas sociedades, foi necessário a implementação de garantia a seus titulares, culminando, no Brasil, na LGPD.

Como resposta à problemática central levantada, verifica-se que a possibilidade da existência de alienação de banco de dados pessoais, mediante consentimento do titular, não encontra impedimentos, à primeira vista, no texto normativo da LGPD.

Contudo, observa-se uma vasta gama de obstáculos à implementação concreta de tal mercantilização sendo o consentimento o maior deles. A possibilidade de existência de vícios nesse é preocupação latente. Assim, o erro e a ignorância são vistos como os maiores entraves, dado que, quando se considera os conhecimentos do homem médio sobre privacidade e dados, esses se mostram insuficientes para que o consentimento dado não se torne vazio.

Ainda, resta comprovado que o consentimento encontra óbices extra-individuais, principalmente no tocante às formas de colheita dele. Essa seria majoritariamente feita através de T&C's, contratos de adesão, que são constatados como escrupulosamente elaborados a fim de diminuir as possibilidades do usuário de conhecer seus direitos básicos, muitas vezes dando interpretações ilegais às cláusulas. Deduz-se que tal fato é agravado pela extensão titânica desses contratos, o que, aliada com sua linguagem extremamente complexa, impossibilita a compreensão, na integralidade, do que está em jogo em dada relação jurídica. Desse modo, é formulado uma posição no sentido de um exame minucioso do judiciário nos casos fáticos, protegendo, de forma enérgica, a parte hipossuficiente do negócio jurídico.

REFERÊNCIAS

BBC. **Norway consumer body stages live app terms reading**. BBC, 2016. Disponível em: https://www.bbc.com/news/world-europe-36378215. Acesso em: 15 jun. 2020.

BIONI, Bruno Ricardo. **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. Relatório de Pesquisa, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Forense, 2018.

ISSN 2594-4991
ISBN 978-65-5615-456-5

BODIN DE MORAES, M. C. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica.com**, v. 8, n. 3, p. 1-6, 15 dez. 2019.

BORAK, Masha. **Wearing a mask won't stop facial recognition anymore**. Abacus, 2020. Disponível em: https://www.scmp.com/abacus/tech/article/3052014/wearing-mask-wont-stop-facial-recognition-anymore. Acesso em: 08 jun. 2020.

BRADSHAW, Simon; MILLARD, Christopher; WALDEN, Ian. Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. **International Journal of Law and Information Technology**, v. 19, n. 3, p. 187-223, 2011.

BRASIL. Lei 13.709/2018. **Lei Geral de Proteção de Dados**. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 5 jun. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 jun. 2020.

BRASIL. **Lei n.° 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 09 jun. 2020.

BRASIL. **Lei 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 19 jun. 2020.

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

CREEMERS, Rogier**. China's Social Credit System**: an evolving practice of control. 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792. Acesso em: 18 jun. 2020.

DA SILVEIRA, Sergio Amadeu. **Tudo sobre tod@ s**: Redes digitais, privacidade e venda de dados pessoais. Edições Sesc, 2017. Não paginado.

DUNDLEY, Lauren. **China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash**. The Diplomat, 2020. Disponível em: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/. Acesso em: 18 jun. 2020.

EUROPA, **General Data Protection Regulation**. Bruxelas, 2018. Disponível em: https://gdpr-info.eu/. Acesso em: 08 jun. 2020.

FOUCAULT, Michel. **Vigiar e punir**. Leya, 2014.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A lei geral de proteção de dados pessoais e suas repercussões no Direito brasileiro**. Revista dos Tribunais, 2019.

ISSN 2594-4991
ISBN 978-65-5615-456-5

GOOGLE. Transparência de Dados. **Google**, 2020. Disponível em: https://safety.google/privacy/data. Acesso em: 19 jun. 2020.

HUXLEY, Aldous. **Admirável mundo novo**. Globo Livros, 2014.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **PNAD Contínua TIC 2018: Internet chega a 79,1% dos domicílios do país**. 29 abr. 2020. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/27515-pnad-continua-tic-2018-internet-chega-a-79-1-dos-domicilios-do-pais. Acesso em: 12 jun. 2020.

JOHNSTON, Matthew. **How Facebook Makes Money**. Investopedia, 2020. Disponível em: https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp#:~:text=Facebook%20breaks%20down%20its%20revenue,separate%20breakdown%20for%20net%20income. Acesso em: 19 jun. 2020.

LÔBO, Paulo. **Direito Civil - Parte Geral**. 6. ed. São Paulo: Saraiva, 2017.

MAGALHÃES, Rodrigo Almeida; DIVINO, Sthéfano Bruno Santos. A proteção de dados da pessoa jurídica e a Lei 13.709/2018: reflexões à luz dos direitos da personalidade. **Scientia Iuris**, v. 23, n. 2, p. 74, 2019.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust de-anonymization of large sparse datasets**. Austin, 2008. Disponível em: https://www.cs.cornell.edu/~shmat/shmat_oak08netflix.pdf. Acesso em: 09 jun. 2020.

NOSEDIVE (temporada 3, ep. 1). **Black Mirror**. Direção: Joe Wright. Produção de: Charlie Brooker. Netflix, 2016. Streaming (63 min).

ORWELL, George. **1984**. Companhia das Letras, 2009.

RIO GRANDE DO SUL. Tribunal de Justiça do Rio Grande do Sul. **Apelação Cível Nº 70060118239**. Relator: Paulo Roberto Lessa. Porto Alegre, 31 jul. de 2014. Disponível em: https://www.conjur.com.br/dl/tj-rs-nega-apelacao-consumidora.pdf. Acesso em: 19 jun. 2020.

RODRIGUES, Juciana. **Anonimização como forma de proteção de dados**. Associação Brasileira de Ciência de Dados, 2020. Disponível em: https://abracd.org/anonimizacao-como-forma-de-protecao-de-dados/. Acesso em: 09 jun. 2020.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge**: improving decisions about health, wealth, and happiness. Penguin, 2009.

THEFIS TEAM. Is Google Advertising Revenue 70%, 80%, Or 90% Of Alphabet's Total Revenue?. **Forbes**, 2019. Disponível em: https://www.forbes.com/sites/greatspeculations/2019/12/24/is-google-advertising-revenue-70-80-or-90-of-alphabets-total-revenue/#3b9418844a01. Acesso em: 19 jun. 2019.

VENOSA, Sílvio de Salvo. **Direito Civi l** – Parte Geral.18. ed. São Paulo: Atlas, 2018. v. 1.

ISSN 2594-4991
ISBN 978-65-5615-456-5

YONG, Ed. **A popular algorithm is no better at predicting crimes than random people**. The Atlantic, p. 55064-6, 2018. Disponível em: https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/. Acesso em: 08 jun. 2020.