A MANIPULAÇÃO DAS INFORMAÇÕES E O PERIGO À DEMOCRACIA: A AMEAÇA OFERECIDA PELO ACESSO IRRESTRITO A DADOS PESSOAIS

THE MANIPULATION OF INFORMATION AND THE DANGER TO DEMOCRACY: THE THREAT OFFERED BY THE UNRESTRICT ACCESS TO PERSONAL DATA

Devilson da Rocha Sousa

Graduado no Curso de Direito da FAE Centro Universitário. Mestrando em Direito da União Europeia pela Universidade do Minho - (Uminho) em Portugal. Mestrando em Direito pela Universidade de Santa Cruz do Sul (UNISC) com bolsa CAPES, sob a orientação do professor Clovis Gorczevski, Pós Doutor em Direito pela Universidad de Sevilla e Mestrando em Direito da União Europeia pela Universidade do Minho – Portugal, sobre a orientação do professor Dr. Pedro Froufe.
E-mail: Devilsonsousa@hotmail.com.

Clóvis Gorczevski

Professor de Direitos Humanos e Fundamentais do PPGD – Mestrado e Doutorado em Direito da Universidade de Santa Cruz do Sul – UNISC (Santa Cruz do Sul-RS, Brasil). Pós-doutor pela Universidad de Sevilla (2007) e pela Universidad de La Laguna (2011).
E-mail: clovisgor@gmail.com.

Recebido em: 01/05/2019
Aprovado em: 27/04/2020

RESUMO: Diante da capacidade crescente que algumas empresas têm em fazer o tratamento de dados pessoais e com isso manipular as informações acessadas por vários indivíduos, no presente artigo são apresentadas e investigadas as medidas e alternativas que o Brasil tem perseguido para enfrentar esta problemática. Com foco especial na recém criada Lei Geral de Proteção de Dados – LGPD, Lei nº 13.709 de 2018, a abordagem do tema se dará por meio do método hipotético-dedutivo e tem como objetivo demonstrar que o Brasil ainda está, mesmo com a criação desta lei, muito longe de possuir mecanismos eficientes de combate de uma problemática que oferece graves riscos à sua ainda embrionária democracia e que essa temática só pode ser melhor enfrentada quando tratada a nível global.

Palavras-chave: Dados pessoais. Democracia. Informação.

ABSTRACT: In view of the increasing capacity of some companies to process personal data and manipulate the information accessed by several individuals, this article presents and investigates the measures and alternatives that Brazil has been pursuing to address this problem. With an special focus on the recently created General Law on Data Protection - LGPD, Law nº 13.709 of 2018, the approach of the topic will be given through the hypothetical-deductive method and aims to demonstrate that Brazil is still, even with the creation of this law, far from having efficient mechanisms to combat a problem that poses serious risks to its still embryonic democracy and that this theme can only be better dealt with when treated at a global level.

Keywords: Personal data. Democracy. Information.

SUMÁRIO: Introdução. 1 O acesso a informação como um dos pilares fundamentais para a democracia. 2 O acesso a dados pessoais como principal meio de manipulação de informações. 2.1 A Lei 13.709 de 2018 e suas nuances. 3 A necessidade de uma good governance global como alternativa para um maior controle pelos estados. Conclusão. Referências.

INTRODUÇÃO

Nunca o ser humano esteve tão bem informado e possuiu de forma tão acessível, em sua mão a um simples toque, uma imensidão de informações e notícias, dos mais variados tipos e das mais variadas fontes. A globalização e as novas tecnologias, nos locais onde elas já se fazem presentes, puseram fim à quase totalidade das limitações territoriais, financeiras, ideológicas e materiais que muitas vezes impediam a população em geral de ter acesso a meios informativos.

Tendo em vista que estar bem informado e possuir meios acessíveis e amplos de obtenção desta informação é fundamental para qualquer cidadão exercer de forma plena e adequada seus direitos, bem como, possibilitar uma participação popular mais efetiva e eficiente, aspectos fundamentais para a manutenção da Democracia e do próprio Estado Democrático de Direito, mais presumível fosse que se estivesse em um momento da história marcado especialmente pela ampliação, em termos qualitativos e quantitativos, destas capacidades, assim como pelo aprofundamento e a ampliação da democracia. Entretanto, o que se tem visto nos últimos anos vem de encontro a toda esta evolução informática possibilitada pelas mais diversas tecnologias.

Tem sido cada vez mais comum o noticiário acerca da forma como determinadas populações se deixaram influenciar, quer seja por um estruturado sistema de notícias cujo único fim é manipulá-las, quer seja pelo acesso, compartilhamento e divulgação de notícias projetadas unicamente para a formação de determinadas opiniões e preferências. A recente eleição de Donald Trump como presidente dos Estados Unidos e a histórica decisão do Reino Unido de sair da União Europeia, um movimento conhecido como Brexit, tiveram influência direta deste fenômeno[1], tendo inclusive ensejado investigações por parte dos órgãos de controle destes países.

No Brasil, como não poderia deixar de ser, recentes acontecimentos históricos, tais como as manifestações que sacudiram o país em 2013, o *impeachment* da ex-presidente Dilma Rouseff[2] e as recentes eleições presidenciais, também foram, em maior ou menor medida, afetados por uma quantidade considerável de informações manipuladas[3]. Tal fenômeno tomou proporções tão grandes que a própria Organização dos Estados Americanos – OEA, em missão ao Brasil em outubro de 2018 para acompanhamento das últimas eleições presidenciais, emitiu declarações acerca da preocupação e da falta de preparo das instituições tradicionais para lidar com esta problemática[4].

[1] Em recente artigo publicado na revista Media & Jornalismo intitulado "Fake News Nas Redes Sociais Online: Propagação e Reações à Desinformação Em Busca de Cliques" Caroline Delmazo e Jonas C.L. Valente trazem dados e informações importantes acerca do impacto que as informações manipuladas e direcionadas tiveram na eleição de Donald Trump e na votação do Brexit.

[2] Na semana que antecedeu a votação da abertura do processo de Impeachment da então presidenta Dilma Rousseff: três das cinco notícias mais compartilhadas no Facebook eram falsas, de acordo com o Grupo de Pesquisa em Políticas Públicas de Acesso à Informaçã o da Universidade de São Paulo (USP), que investigou o desempenho de 8.290 reportagens, publicadas por 117 jornais, revistas, sites e blogs noticiosos entre 12 a 16 de abril de 2016 (Lavarda, Sanchotene & Silveira, 2016, p.1).

[3] Para miores esclarecimentos acerca deste ponto, conferir as matérias publicadas no site de notícias Uol em 24 de julho de 2018.

[4] Em entrevista concedida ao site UOL a ex-presidente da Costa Rica e chefe de missão da OEA na eleição brasileira, Laura Chinchilla afirmou que a disseminação de notícias falsas e a manipulação de informações é um fenômeno sem

Se quer sustentar neste trabalho que a despeito de todo este cenário, não se afigurado adequado ou mesmo suficiente os esforços realizados pelo Brasil no sentido de prevenir e combater tais fenômenos, possibilitados em grande medida pelo acesso e manipulação aos dados pessoais de populações inteiras, e que mesmo a Lei nº 13.709 de 2018, que surgiu como principal ferramenta nesta luta, carece de maior efetividade.

A metodologia de abordagem dos temas sinalizados neste trabalho será a hipotético-dedutiva, partindo da demarcação teórica e pragmática do cenário atual e de seus riscos ao Estado Democrático de Direito, para então investigar o problema de pesquisa que orbitará no questionamento de como compatibilizar com os fundamentos tradicionais do Estado e os avanços que a tecnologia vem propiciando, assim como, em que medida se revelam inadequadas as soluções até então surgidas no horizonte brasileiro e demonstrando que para o efetivo tratamento desta problemática uma cooperação entre Estados – internormatividade, e uma *good governance* são fundamentais.

1 O ACESSO A INFORMAÇÃO COMO UM DOS PILARES FUNDAMENTAIS PARA A DEMOCRACIA

As novas conjecturas estatais, econômicas e do próprio direito, já não são as mesmas que as enfrentadas anteriormente, e nessa perspectiva o Estado cada vez mais vem sendo chamado a responder acerca de problemáticas que há o pouco tempo não eram nem mesmo percebidas por seus teóricos e estudiosos.

Como não poderia deixar de ser, os novos problemas que se afiguraram no horizonte têm demandado um esforço sobre-humano dos governos e das instituições, que em muitas oportunidades não sabem sequer como lidar com estas novas conjecturas e mudanças. O fenômeno da manipulação das informações e da própria *fake news*[5] estão aí para provar essa dificuldade no tratamento de novas temáticas.

É de se observar que o acesso à informação, fator essencial para a formação da opinião e para tomada de decisões, anda de mão dadas com a democracia, não havendo que se falar nesta última em locais onde a primeira inexiste ou é controlada e/ou filtrada pelo próprio Estado. Além de possibilitar escolhas mais qualificadas e razoáveis, o acesso à informação é indispensável na perspectiva individual do ser enquanto integrante de uma sociedade e formador do Estado, uma vez que busca pela garantia de seus direitos passa antes pela ciência destes, ou seja, o acesso à informação é um direito que antecede e possibilita os outros.

Neste tocante, importa destacar que é pressuposto fundamental para qualquer Estado Democrático de Direito assegurar a seus cidadãos condições e garantias reais que os possibilitem formular uma opinião livre e esclarecida, não bastando para este fim a simples atribuição do direito de participação direta ou indireta na tomada de decisões políticas e governamentais, ou mesmo, a existência de regras procedimentais que organizem o jogo democrático, como bem observado por Norberto Bobbio (BOBBIO, 1981, pág. 40).

Aléxis de Tocqueville em seu livro "A democracia na América" já apontava, quando ao observar a florescente democracia estadunidense, que uma imprensa livre, naquele momento o único meio dos cidadãos obterem informações, era "o principal e, por assim dizer, o elemento constitutivo da liberdade"(TOCQUEVILLE, 1998, Pág. 209 e ss). Se Tocqueville fosse vivo hoje, é provável que sua observação incluísse os mecanismos de controle a dados pessoais e o combate

precedentes que tem preocupado a missão da OEA (Organização dos Estados Americanos) que está no Brasil para observação das eleições.

[5] Allcott e Gentzkow (2017) definem *fake news* como "artigos noticiosos que são intencionalmente falsos e aptos a serem verificados como tal, e que podem enganar os leitores" (p.4, tradução própria). Guess, Nyhan e Reifler (2018) falam de "um novo tipo de desinformação política" marcada por uma "dubiedade factual com finalidade lucrativa" (p. 2).

a manipulação de informações como outro ponto fundamental para esta liberdade. Conforme Tocqueville (1998, Pág. 215):

> Quando se concede a cada qual um direito de governar a sociedade, cumpre reconhecer-lhe a capacidade de escolher entre as diferentes opiniões que agitam seus contemporâneos e apreciar os diferentes feitos cujo conhecimento pode guiá-lo. A soberania do povo e a liberdade de imprensa são, pois, duas coisas inteiramente correlativas.

O método democrático se configura como um sistema institucional que busca e viabiliza a tomada de decisões políticas pelo povo, sendo que todos os indivíduos adquirem o poder e a prerrogativa de decidir acerca do destino do Estado. A tomada dessas decisões só pode ser eficiente e atender aos anseios de uma autêntica democracia quando os cidadãos puderem compatibilizar seus posicionamentos e formar sua opinião a partir do acesso a diferentes meios informativos.

Do mesmo modo, tanto as novas teorias da democracia contemporânea quanto a teoria da democracia participativa fazem a defesa do argumento da necessidade de que os indivíduos que estejam inseridos nestes sistemas devam receber de alguma forma uma espécie de "treinamento" de exercício da democracia, não devendo este treinamento se limitar ao processo político nacional.

Nesta mesma perspectiva a teoria da democracia participativa sustenta que esta experiência de participação de alguma forma possibilita e torna o indivíduo psicologicamente melhor preparado para participar de forma mais efetiva no arranjo democrático, esse "treinamento" só poderá ser feito quando o acesso a informações e o entendimento acerca do Estado são possibilitados de forma ampla a todos os cidadãos.

Já segundo a concepção republicana, o status dos cidadãos não pode ser determinado unicamente por meio de um modelo de liberdades negativas que eles podem reivindicar como pessoas em particular. Os direitos de cidadania, direitos de participação e comunicação política são, em primeira linha, direitos positivos e essenciais para a prática democrática (PATEMAN, 1992, Págs. 65).

Habermas (2004, Pág. 279) defende a construção de uma esfera pública autêntica e cidadã a partir das instituições da sociedade civil e de movimentos sociais emancipacionistas, onde é possível estabelecer um espaço social de debate no qual vigore a razão comunicativa, ou seja, aquela que se desenvolve intersubjetivamente, livre da dominação ideológica do sistema e por meio do exame público dos argumentos expostos, só sendo possível quando os cidadãos, dentre outras coisas, possuem acesso a meios informativos eficientes e imparciais. Assim sendo, os meios de comunicação são fundamentais para a conquista de uma razão comunicativa, que por sua vez é imprescindível para o exercício da democracia.

É de se observar que atualmente há uma quantidade cada vez maior de meios de acesso e da própria informação, que é difundida pelas mídias escritas, televisivas e, sobretudo, eletrônicas. Essa quantidade massiva de informações tem o poder de causar, paradoxalmente, a desinformação e a ignorância geral, na medida em que não há nenhum filtro ou controle do que se é noticiado e difundido.

A própria mídia tradicional também por vezes tem relevante papel no processo de manipulação e, na definição feita por Habermas (2004, Pág. 279), "na colonização do mundo da vida", ao definir por critérios próprios qual será a abordagem da realidade social que tomará. Deste modo, se de um lado o acesso e o intercâmbio de informações são ferramentas úteis à emancipação política e democrática, por outro tem se tornado cada vez mais difícil que essa informação não gere desinformação e manipulação.

Acerca deste fato, não se pode fugir a mente, como bem observa Dowbor, (2017, pág. 11) que os Estados Unidos da América, uma das mais bem informadas e instruídas nações do mundo, se deixou levar e influenciar em grande parte por informações que posteriormente se revelaram

incorretas ou mesmo falsas[6]. Fica evidente assim que tão importante quanto o acesso a informações é a sua a real capacidade informativa e veracidade.

Por este motivo, e considerando o fato de que em qualquer sociedade, por mais primitiva ou rudimentar que ela seja, a informação possui a capacidade de ditar os rumos da política, da economia, bem como, de moldar os comportamentos sociais, é cada vez mais imprescindível a sua vigilância e o seu compromisso com a verdade. Por certo o Estado, para sua própria sobrevivência, precisa de mecanismos que sejam eficientes na tarefa de combater a informação que gere desinformação e transforme os cidadãos em massa de manobras a serviço de uns poucos ou de interesses privados.

Mas como compatibilizar isso em uma sociedade em que cada vez mais o acesso à informação se dá por meios não tradicionais e que não têm, ao menos em regra, quaisquer formas de controle ou comprometimento com os interesses públicos? É essa resposta que se objetivará responder nos próximos tópicos.

2 O ACESSO A DADOS PESSOAIS COMO PRINCIPAL MEIO DE MANIPULAÇÃO DE INFORMAÇÕES

A sociedade contemporânea é corriqueiramente nomeada como a sociedade da informação, tamanha a capacidade informativa que possui e a importância que esta tem para a política, economia e tecnologia. Como visto acima, atualmente tão importante quanto o acesso à informação, é saber sua veracidade e origem.

Os avanços tecnológicos que possibilitaram conectividade em tempo real na quase totalidade do globo terrestre também trouxeram novos desafios e problemas, em especial os que se referem ao acesso, por parte de plataformas eletrônicas, redes sociais, buscadores de internet e banco de dados, a informações muitas vezes de caráter sigiloso e que só dizem respeito ao particular, ou seja, que são informações de cunho particular.

Para se ter uma ideia do potencial destas informações, por meio do rastreio de gastos nos cartões de crédito as suas operadoras conseguem traçar um perfil extremamente específico de seus usuários, sendo inclusive possível saber sua movimentação física, suas preferências pessoais e seus planos. De igual modo, o *Facebook* e o *Instagram* têm acesso a todas as informações presentes nos *smartphones* de seus usuários, suas buscas na internet, seus gostos, rede de amigos, assuntos de interesse e etc, dados suficientes para controlar e manipular qualquer pessoa.

O resultado inevitável dessa coleta massiva é a criação de um banco de dados extenso e detalhado acerca dos indivíduos, assim como a possibilidade de monitoramento eletrônico praticamente durante todas as horas do dia. Tais fatos têm causado grandes preocupações quando vislumbrados a partir da ótica do direito à privacidade e do direito à proteção de dados pessoais dos indivíduos, conforme bem destaca Bioni (2019, Pág, 127).

O poder, aqui entendido como capacidade de impor a outros vontades e desejos alheios, que estas informações oferecem é tão grande que os escândalos de furto de dados têm ficado cada vez mais comuns[7], e fica fácil perceber o porquê disso, com o acesso irrestrito a todas estas informações companhias conseguem mapear e direcionar informações a públicos específicos, de modo a direcioná-los a escolha desde um simples produto ou serviços, até a políticos, partidos, sistemas de governo, políticas sociais e por ai em diante.

[6] Dowbor destaca que em que pese a evidente capacidade Dos cidadãos dos EUA se informarem por inúmeros meios e terem facilidade para acessar as mais diversas informações, bem como possuírem condições educacionais acima da média mundial, boa parte destes cidadãos se deixaram manipular por informações falsas ou mesmo que não possuíam qualquer comprovação ou embasamento teórico (DOWBOR, 2019, Pág., 11).

[7] Conforme matérias publicadas recentemente no site de Notícia UOL, empresas como Facebook, C&A e Boa Vista SPC foram alvo de ataques cibernéticos que tinham como fim o furto de informações.

O maior exemplo deste poder pode ser mensurado com o caso da Cambridge Analytica nos Estados Unidos, a empresa teve acesso por meios ilegais a dados sigilosos de mais de 50 milhões de cidadãos estadunidenses e os utilizou para direcionar mensagens ou mesmo criar notícias falsas contra a candidata Hillary Clinton. A Cambridge integrou a campanha de Donald Trump e muitos analistas atribuem a sua vitória a atuação desta empresa[8].

Acerca deste ponto SILVEIRA (2018, pág. 23) defende:

> De resto, para que servem as eleições democráticas se os algoritmos de aprendizagem antecipam em quem vamos votar? O escândalo envolvendo o Facebook e a Cambridge Analytica revela em que medida é possível, em democracia, promover a manipulação do eleitorado socorrendo-se de dados obtidos ilegitimamente (87 milhões de internautas tiveram os seus dados negociados, sem consciência dos visados, para os efeitos de manipulação eleitoral). Como sabemos, a partir da recolha de informação de 300.000 internautas (através de um inquérito/jogo), o Facebook permitiu a apropriação indevida de dados pessoais de milhões de pessoas. No Reino Unido, tanto quanto se sabe, 1.1 milhão de cidadãos foram alvo de tal apropriação. Ora, se a diferença entre o Remain e o Exit foi de 1.3 milhões de votos, é legítimo presumir que a manipulação levada a efeito pode ter sido determinante nos resultados do referendo britânico.

Diante deste cenário é cada vez mais latente a forma como uma expressão livre, seja em relação a preferências políticas ou outros assuntos de interesse geral, é dificultada e tolhida, fazendo com que a real capacidade dessa expressão não se repercuta nos processos decisórios que afetam o quotidiano dos cidadãos.

Por conta disso, a temática da proteção de dados tem ganhado cada vez mais destaque em todo o mundo, recentemente o Tribunal de Justiça da União Europeia – TJUE, em um julgado conhecido como "caso Facebook", esclareceu e pôs limites, com base na diretiva 95/46/CE[9], sobre a transferência e o tratamento dos dados de uma pessoa alocados em servidores de outros países[10]. A diretiva 2016/680[11] e o General Data Protection Regulation – GPDR de igual forma vem tentar possibilitar uma melhor prevenção e busca impedir eventuais manipulações de informações a partir do acesso a estes dados, ou mesmo, a utilização destes para fins diversos daqueles pelo qual foi obtida.

Do mesmo modo, do outro lado do atlântico os EUA têm buscado formas de prevenir e combater a manipulação de informações por meio do acesso irrestrito que determinadas companhias têm a dados pessoais, bem como limitar a sua utilização. O Clarifying Overseas Lawful

[8] Tais informações foram extraídas a partir da matérias publicadas em site de notícina nacionais e internacionais, em especial portal de notícia G1 e a Rede Britânico BBC.

[9] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares despende um tratamento especial a questão Do tratamento de dados pessoais e à livre circulação desses dados (JO L 281, p. 31).

[10]No acórdão do processo C-362/14 o Tribunal de Justiça declara inválida a decisão da Comissão Europeia que constatou que os Estados Unidos asseguram um nível de proteção adequado dos dados pessoais a ele transferidos. No mesmo acórdão o tribunal salientou que uma regulamentação que não prevê nenhuma possibilidade de os particulares acionarem vias de direito para ter acesso a dados pessoais que lhes dizem respeito, ou obter a retificação ou a supressão desses dados, infringe o conteúdo essencial do direito fundamental a uma tutela jurisdicional efetiva, possibilidade esta que é inerente à existência de um Estado de Direito.

[11] A diretiva 2016/680 do Parlamento Europeu e do Conselho Europeu, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

Use of Data Act[12], o CLOUD Act, uma lei federal sancionada em 23 de março de 2018 é a mais recente alternativa para este fim.

No Brasil, a questão do acesso a informações e dados pessoais já vem sendo estudada há algum tempo, contudo voltada muito mais ao acesso destas por parte de órgãos públicos e do próprio fisco do que a forma de seu tratamento e proteção. Em artigo publicado na revista Nomos da Universidade Federal do Ceará, Gomes, Abraham e Pereira (2016, pág. 339) já asseveravam sobre os limites e interpretações delineados pelo Supremo Tribunal Federal – STF, em relação ao sigilo bancário e a privacidade do cidadão.

Por parte do governo brasileiro foi apenas com a instituição da Lei nº 13.709 de 2018 que esta temática realmente começou a ser tratada de forma mais específica e detalhada, uma vez que a legislação até então existente abordava apenas questões satélites e não o tratamento de dados especificamente[13] é impostante destacar que a figura do *Habeas Data*, ainda que prevista no texto Constitucial, não oferece mecanismos suficientes ao combate desta problemática. A lei procura tratar e disciplinar as regras para a proteção dos dados pessoais coletados, tanto pelo meio convencional quanto no digital, por pessoa natural ou por pessoa jurídica de direito público ou privado. [14].

Ainda, cumpre observar que antes desta lei a questão de dados pessoais era tratada de forma muito esparça e genérica pela legislação, exemplos claro é a Lei nº 11.419/2006, que instituiu o processo eletrônico e que reservou um tópico para tratar da guarda e segurança de dados pessoais, e a Lei nº 12.682/12 que dispõe da elaboração e o arquivamento de documentos em meios eletromagnéticos.

O Tribunal Superior Eleitoral – TSE por meio da Resolução nº 23.551 de 2017 também buscou tratar do assunto, contudo, muito mais voltada para a propagação de *fake news* e propaganda eleitoral, o que ainda assim foi insuficiente para impedir a disseminação destas.

2.1 A Lei 13.709 de 2018 e suas nuances

O princípio norteador da lei está assentado na perspectiva de que toda pessoa natural deve ter assegurado a titularidade de seus dados pessoais e a ciência quando do seu tratamento, uma vez que sem isso o exercício dos direitos fundamentais de liberdade, de intimidade e de privacidade estariam em risco, além de ser fator essencial para "o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018)

Nestas perspectiva, a lei também obriga que qualquer pessoa física ou jurídica que faça o tratamento, ou tenha acesso a estas informações de forma autônoma, colha o consentimento dos seus titulares, devendo ainda ser garantido a estes a possibilidade de revogação desta autorização a qualquer momento.

Independente do meio de coleta, a Lei de proteção de dados será aplicada se: a) a operação de tratamento for realizada em território nacional; b) a atividade de tratamento tenha por objetivo

[12] Em que pese ser um dos seus objetivos seja o combate e o controle de informações por parte do governo dos EUA, o Cloud Act tem recebido diversas críticas, em especial por deliberadamente outorgar, sem a necessidade de uma autorização judicial, as forças policiais a capacidade de obter e ter acesso a informações particulares, com a simples justificativa de servir para fins investigatórios.

[13] Apesar do seu objetivo grandioso, a lei recebeu diversas críticas, em especial por ser considerada uma cópia piorada do General Data Protection Regulation Europeu e carecer de mecanismos de aplicação autônomos, uma vez que a lei atribui algumas funções chavesa um órgão de controle que se quer havia sido instituído, e que por uma falha legislativa ainda estava sem previsão de instituição.

[14] Devido a uma falha no processo legislativo, o Presidente vetou os artigos 55 a 59 do Capítulo IX relativos à criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que seriam os órgãos responsáveis por supervisionar e impor o cumprimento da LGPD. A perspectiva é que presidente envie outro projeto de lei ao Congresso para corrigir esta falha assim permitir que a ANPD seja devidamente estabelecida dentro do período de carência de 18 meses.

a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e c) os dados pessoais objeto do tratamento tenham sido coletados no território nacional, sendo considerado coletado em território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Acerca do aspecto da territorialidade, Pinheiro (2018, Pág. 113) destaca que a lei também prevê aplicação extraterritorial de suas disposições, bastando para tanto que os dados pesoais tratados em outro país tenham sido coletados dentro do território brasileiro, ou o objeto de transação comercial, quer seja esta consistente em oferta de bens ou de serviços, tenha ocorrido dentro do território nacional.

A lei traz ainda a diferenciação entre: a) dados pessoais, entendido como toda informação relacionada a pessoa natural identificada ou identificável; b) dado pessoal sensível que é dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; e c) dado anonimizado que é o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Já o titular é toda pessoa natural a quem se referem os dados pessoais que serão objeto de tratamento.

Aqui cumpre destacar, mais uma vez tendo em consideração os ensinamentos de Bioni (2019, Pág. 68), que o conceito de dado pessoal é elemento central para a discussão sobre a legislação, não devendo este ser relacionado apenas com a privacidade, vez que transita e interfere em outras direitos da personalidade, podendo mesmo a proteção de dados pessoais ser considerada como elemento central de um novo direito da personalidade, direito este vinculado a toda e qualquer informação de origem no e do indivíduo.

Por tratamento a lei entende toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O artigo 6º por meio de seus incisos determina ainda que deverá ser informado ao titular o propósito do tratamento dos seus dados e em havendo mudanças na sua finalidade, sendo estes não compatíveis com o consentimento original, o controlador de tratamento, pessoa física ou jurídica responsável pelo tratamento dos dados, deverá informar previamente o titular sobre as mudanças ocorridas, podendo o titular revogar o seu consentimento caso discorde das alterações. Da mesma forma impõe que deve haver limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

É garantido ainda aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como, sobre a integralidade de seus dados pessoais. Em relação a qualidade há ainda a obrigação de haver garantia aos titulares de exatidão, clareza e relevância dos dados em tratamento, assim como a atualização destes de acordo com a necessidade e para o cumprimento de sua finalidade.

A transparência é outro ponto abordado. O inciso VI do artigo 6º traz a determinação de que seja possibilitado aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos controladores de tratamento, sendo observados eventuais segredos comerciais e industriais.

A segurança foi outro ponto que mereceu uma redação detalhada. Segundo o mesmo artigo 6º, os agentes responsáveis pelo tratamento deverão utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, bem como, devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento destes dados.

Os dados tratados sob nenhuma forma poderão servir a fins discriminatórios ilícitos ou abusivos, devendo ainda o controlador adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas[15].

O legislador incluiu um capítulo inteiro na lei para tratar especificamente sobre segurança e das boas práticas[16], o que demonstra sua preocupação com esta questão. Do mesmo modo, para atender aos requisitos da lei, e como já mencionado, o tratamento dos dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular, salvo nos casos em que os dados já se tornaram manifestamente públicos pelo titular, sendo resguardados porém os direitos do titular e os princípios previstos na lei[17].

Em se tratando de meios digitais, onde a grande parte dos dados hoje são coletados, os meios pelos quais o titular consentirá em fornecer seus dados deverão ser muito bem estruturados e serem capazes de garantir a integridade, autenticidade e disponibilidade dos registros. Acerca deste ponto é importante ser observado que, em se tratando de registros eletrônicos, o artigo 441 do Código De Processo Civil – CPC, dispõe que a produção e a conservação de documentos eletrônicos observarão a legislação específica. Neste caso, há duas leis que tratam deste ponto, a Lei nº 11.419/2006, que instituiu o processo eletrônico, e a Lei nº 12.682/12, que trata da elaboração e o arquivamento de documentos em meios eletromagnéticos[18].

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse e com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou responsável legal.

Além disso, é também assegurado ao titular a possibilidade de transferência de seus dados para outro controlador de tratamento, neste caso, pelo próprio espírito da lei, o controlador cedente deverá transferir de todos os seus registros os dados da pessoa que solicitou a transferência, não devendo manter consigo qualquer *back up* ou rastreabilidade destes.

Ao término do tratamento, todos os dados coletados deverão ser eliminados, o que se vê mais como um desejo do que como algo que realmente vai ser seguido, afinal de contas, não há mecanismos na lei, ou por parte do próprio governo, com capacidade de assegurar esta ação. Ainda, seria inocência imaginar que uma imobiliária, ou mesmo uma empresa que vende seus produtos a consumidores diversos, apagara de todos os seus registros os dados de clientes que migraram para outras empresas ou que encerraram seu relacionamento.

No tocante à transferência internacional de dados, o artigo 33 da lei estabelece de forma exaustiva as situações em este será permitido, a lei foi omissa entretanto em relação a responsabilidade em território nacional quando do uso indevido ou mesmo em relação ao vazamento ou perda destas informações por parte do controlador que as recebeu em outro país. Pelo próprio espírito da lei se pode concluir que o controlador responsável pela transferência do Brasil para o exterior será o responsável, salvo quando transferida para atingir interesse público ou quando autorizada por autoridade estatal, por este vazamento.

Outro ponto de destaque é o capítulo VI onde foram definidas as figuras do controlador, operador e encarregado, da mesma forma que a lei de proteção de dados da União Europeia. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; o operador a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador e o

[15] Nos termos do estabelecido no inciso IX do artigo 6 da Lei 13.709/2018.
[16] Nos termos do estabelecido no Capítulo VII da Lei 13.709/2018, mais precisamente a partir do artigo.
[17] Nos termos do estabelecido no § 4º do artigo 7º da Lei 13.709/2018 .
[18] A Lei nº 11.419/06, estabelece nos artigos 11 e 12, respectivamente, que deve ser garantida a origem do documento e de seu signatário, bem como que os documentos eletrônicos devem ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, já a lei nº 12.682/1, trata desta questão em seu artigo 3º.

encarregado é a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional.

Fica a cargo do operador a realização do tratamento dos dados segundo as instruções fornecidas pelo controlador ou seja, o controlador deverá definir uma politica de segurança da informação devendo verificar com frequência se ele está atendendo a legislação, nos casos de tratamento feito por empresa terceira esta verificação deverá se dar por meio de auditorias. Da mesma forma a lei obriga ao controlador indicar a figura do encarregado, devendo a sua identidade e contato serem divulgadas publicamente.

O artigo 4ºda lei traz as situações em que não serão aplicadas as disposições da Lei nº 13.709. De todas as possibilidades ali dispostas, as do inciso III é que trazem maiores preocupações[19], uma vez que outorgam uma grande margem de isenção para o Estado. Em relação ao inciso III a lei diz que estes casos serão "regidos por legislação específica, que deverá prever medidas ao atendimento do interesse público" (BRASIL, 2018), entretanto, não existe esta legislação específica.

Por fim, resta destacar ainda que os bancos e financeiras, particulares que obtém informações extremamente sensíveis e importantes, ficaram de fora das teias da lei, quer seja por descuido do legislador – o que não se crê, quer seja pelo *lobby* feito por estes quando da elaboração do projeto de lei. Ao deixá-los de fora, a lei tem sua efetividade muito reduzida.

Além disso o veto presidencial que excluiu as sanções administrativas de suspensão parcial ou total do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados pessoais e de proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados praticamente aniquilaram as forças coercitivas da lei.

3 A NECESSIDADE DE UMA *GOOD GOVERNANCE* GLOBAL COMO ALTERNATIVA PARA UM MAIOR CONTROLE PELOS ESTADOS

Conforme já mencionado no presente texto, a tecnologia acabou, ou ao menos diminuiu consideravelmente, a quase totalidade das barreiras de comunicação que limitavam ou impediam as sociedades de avançarem e evoluírem mais rapidamente. Atualmente com apenas um clique é possível superar os limites territoriais dos Estados e transferir dinheiro, informações, notícias, dados e etc., para qualquer lugar do mundo em questões de minutos.

Entretanto, ao mesmo tempo que trouxe facilidades essa revolução tecnológica vem ofertando desafios enormes para um Estado que não acompanha com a mesma velocidade a evolução de sua sociedade[20]. Prova disso é que somente há pouco tempo começaram a surgir as primeiras legislações para tentar por ordem e limites ao compartilhamento e acesso desenfreado a dados e informações pessoais, mesmo este fenômeno já tendo sido sentido há alguns anos.

Se o conceito de democracia digital implicou a utilização de meios eletrônicos de comunicação para potencializar e ampliar a ação dos cidadãos e do mesmo modo controlar os governantes e as instituições públicas, por outro lado esta mesma democracia digital deixou os cidadãos reféns das corporações que possibilitam essa participação digital.

Por este motivo é que o Estado precisa se reinventar de forma a buscar que sua autoridade e interesses se façam presentes além dos seus limites territoriais, isso sem limitar ou mesmo violar

[19] Diz o inciso III do artigo 4º que estão isentas de aplicabilidade da lei os tratamentos realizados para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;

[20] Neste sentido, muito bem destaca Alessandra Silveira ao lecionar que "tudo se agrava atualmente porque as instituições da democracia moderna desenvolveram-se numa época em que a política avançava mais rapidamente que a tecnologia – e, desta forma, conseguia regular e controlar a sua trajetória. Mas deixou de ser assim, sobretudo porque o poder desterritorializou-se". Citação retirada do texto "Mais vale uma Constituição cidadã enclausurada ou uma Constituição cidadã em rede?" ainda não publicado e facultado pela autora.

a soberania e autoridade de outros Estados. Mesmo que paradoxal tal ação é possível através da celebração de acordos com outros Estados e da criação de uma legislação internacional em rede[21].

Tal ação é necessária uma vez que sem integração e cooperação internacional os esforços feitos não só pelo Brasil com por qualquer outro país estarão limitados desde o berço. Isso porque as empresas que têm acesso e fazem o tratamento de dados pessoais da maioria das populações têm filiais e exercem suas atividades a partir de várias localidades.

Um exemplo claro pode ser obtido com o *facebook* a rede social faz o armazenamento da quase totalidade de seus dados na Irlanda do Norte, uma vez que aquele país tem regras mais frouxas sobre esta questão, conforme apontam alguns relatórios do Tribunal de Justiça da União Europeia e da própria Comissão Europeia[22].

Conforme apontado por Dowbor,(2017, pág. 43) a ausência de um sistema de governança adequado tem impactado diretamente na criação de soluções e formas de controle dos gigantes corporativos que têm se apossado do Estado sem que estes se quer se deem conta ou mesmo tenham capacidade de se defender.

Do mesmo modo Zagrabelsky (1992, pág. 199) explica que o poder político e constitucional já não se exerce da mesma forma, uma vez que o poder não tem mais um marco territorial, ou só o tem parcialmente, caracterizando aquilo que se convencionou a chamar de "desterritorizalização do poder".

Uma governança em matéria de proteção de dados a nível global é necessária para que o sistema político nacional não seja reduzido ainda mais a um mero gerente de interesses corporativos ou privados, deixando de ter qualquer representação política frente a um sistema global isento de controles e sem qualquer subordinação.

E quando se fala da necessidade de criação de uma governança global e da imposição de limites à atuação de determinadas corporações em relação ao acesso e tratamento de dados pessoais, não se está querendo impor uma regulação parcial e acrítica por parte dos Estados a exemplo do que acontece em várias ditaduras.

O que se propõe é criação de mecanismos e órgãos de controle que possibilitem limitar o poder de atuação e controle que estas empresas possuem em relação a seus consumidores e usuários. É importante observar que hoje há corporações que possuem dados suficientes para desestabilizar e gerar crises em diversos países, sem que estes possuam se quer formas de combater eventual ação.

A União Europeia, mesmo com todas as limitações e críticas, é até o momento o mais bem-sucedido exemplo desse movimento. A partir de suas diretivas e da atuação de suas Comissões e do TJUE ela têm imposto seguidas limitações e ajustes a empresas que fazem o tratamento de dados de seus cidadãos. Isso se deu especialmente pela consciência de que a ação desenfreada destas empresas revelam um grande risco as democracias de seus Estados-Membros e a própria integração de toda aquela União.

Acerca deste risco HARARI (2015, pág. 12 e ss), na sua obra Homo Deus, tem defendido que o aumento do volume e da velocidade dos dados acessados pelos cidadãos e tratados por corporações podem fazer com que instituições respeitáveis como os partidos políticos, o sistema eleitoral e as próprias assembleias parlamentares percam para alguns a sua importância e acabe por tornarem-se obsoletas ou arcaicas.

[21] O termo legislação em rede cunhado aqui é no mesmo sentido do utilizado por J. J. Gomes Canotilho em: Canotilho e a Constituição dirigente, in Jacinto Nelson de Miranda Coutinho (coord.), Renovar, Rio de Janeiro/São Paulo, 2003.
[22] Mais informações acerca dos relatórios e das observações feitas em relação ao armazenamento dos dados pelo *Facebook* podem ser obtidos no acórdão do TJUE citado na nota de rodapé nº 16.

Segundo SILVEIRA (2018, pág. 23)[23] , em referência ao mesmo autor:

> A democracia e o mercado livre triunfaram porque souberam, sob a alçada das circunstâncias únicas do final do séc. XX, aprimorar o sistema global de processamento de dados, através da sua dispersão em detrimento da concentração. Todavia, no séc. XXI, as estruturas políticas tradicionais já não conseguem processar os dados com a rapidez suficiente a fim de projetarem visões significativas para o futuro.

No cenário sul-americano ainda não há registros de acordos ou pactos celebrados neste sentido, ao que parece, enquanto boa parte dos países estão buscando alternativas a este novo fenômeno e apresentando relatórios acerca dos riscos oferecidos por empresas que tem acesso a tudo no que diz respeito a informações e dados pessoais, regionalmente apenas Brasil, Argentina e Chile se tem debruçado sobre a matéria.

No horizonte já é possível ver as nuvens que prometem causar uma crise ainda não vivenciada pelo Estado e suas instituições, o desafio será este Estado sobreviver a estas novas conjecturas e problemáticas, caso contrário se presenciará o surgimento de um novo arquétipo de poder político, uma vez que não há do que se falar na inexistência ou no esvaziamento da estrutura política.

CONCLUSÃO

O acesso à informação é fundamental para a manutenção de qualquer democracia uma vez que sem estar bem informado o cidadão não pode exercê-la de forma plena e eficiente, os avanços democráticos no decorrer da história se deram, dentro outros fatores, pela difusão da informação e seu acesso amplo.

O aumento a este acesso que a tecnologia proporcionou foi tão grande que atualmente já se fala inclusive em democracia digital, uma vez que esta deu voz a uma imensidão de cidadãos, possibilitou uma maior participação destes e passou a ser utilizada como ferramenta de pressão dos agentes políticos e autoridades públicas.

Entretanto, tão essencial quanto a difusão e o acesso à informação, passou a ser a sua procedência e sua fonte, uma vez que esta passou a servir a um fim oposto ao seu, proporcionando em muitos casos desinformação ou mesmo servindo como meio utilizado para manobrar e direcionar a opinião pública e seus interesses a determinado fim.

Como visto acima, o principal meio pelo qual esta manipulação é feita se dá pelo acesso, incluindo aqui o furto, vazamento ou mesmo a venda, de dados e informações pessoais que muitas empresas possuem acerca de seus usuários ou consumidores. Ao saber as preferências, desejos, círculo de amizades, principais gastos e etc., estas possuem informações suficientes para identificar o perfil, direcionar informações e moldar os interesses dos particulares da forma como bem entenderem.

Tal poder na mão de quantidade enorme de agentes que muitas vezes estão espalhados por diversos países e que possuem ramificação e ligações com vários outros, oferece um risco real a democracia e a estabilidade de qualquer Estado. Por este motivo é que a proteção de dados pessoais se tornou matéria preponderante nas mais diversas ordens jurídicas, com ênfase especial para a União Europeia e sua GPDR.

Do mesmo modo, no cenário nacional a Lei nº 13.709 de 2018 surgiu como a principal ferramenta na busca por uma maior proteção e controle a dados de caráter pessoal e que na grande maioria das vezes são de caráter sigiloso. Em que pese o caro fim a que se destina, a lei carece de

[23] Esta citação foi retirada do texto "Mais vale uma Constituição cidadã enclausurada ou uma Constituição cidadã em rede?" ainda não publicado, mas que foi facultado pela Autora quando do desenvolvimento do presente trabalho.

maior efetividade e operacionalidade uma vez que ao trazer obrigações difíceis de serem acompanhadas por autoridades públicas já nasceu fadada a não atingir seus objetivos.

Além disso, ao trazer expressões genéricas, outorgar obrigações primordiais a uma autoridade que ainda não foi instituída, e até o momento da redação final deste artigo não se sabe se será, e deixar de fora um segmento chave na manipulação de dados pessoais como os bancos e ter algumas de suas sanções retiradas por veto presidencial, a lei de proteção de dados perdeu parte importante de sua efetividade e fim de existir.

Afora todos estes aspectos, cumpre observar que sem uma interligação a nível internacional e a criação de uma *good governance* em matéria de tratamento de dados, a quase totalidade de ferramentas criadas pelos Estados para a proteção destes estarão, desde o seu surgimento carentes de maior alcance e efetividade. É necessário que os Estados se alinhem de forma a buscarem juntos alternativas ao crescente domínio que os agentes que possuem dados pessoais têm em mãos, bem como, criem organismos e mecanismos eficazes no controle e no combate ao uso indevido destas.

Sem esse alinhamento a democracia da forma como concebida hoje corre sérios riscos de inexistir e o próprio Estado se torna presa fácil nas mãos de determinados grupos, passando a servir muita das vezes apenas como gerenciador de seus interesses.

REFERÊNCIAS

BAUMAN, Zygmunt; BORDONI, Carlo. Estado de crise. Editora: Relógio D'Água Editores, Lisboa, 2016.

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

BOBBIO, Noberto. O futuro da democracia (uma defesa das regras do jogo). Trad. Marco Aurélio Nogueira. Rio de Janeiro, Paz e Terra, 1986.

_____. Estado, Governo e sociedade . Para uma teoria geral de política. São Paulo: Paz e Terra, 2005.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018.

CANOTILHO, J. J. Gomes. "Brancosos" e interconstitucionalidade: itinerários dos discursos sobre a historicidade constitucional. 2. ed. Almedina: Coimbra, 2008.

DAHL, Robert A. Sobre a democracia. Tradução de Beatriz Sidou. Brasília : Editora Universidade de Brasília. 2001. Parte II e III.

DOWBOR, Ladislau. A era do capital improdutivo, São Paulo: Autonomia Literária, 2017.

GOMES, Marcus Lívio; ABRAHAM, Marcus; PEREIRA , Vítor Pimentel. "O sigilo bancário e a privacidade do cidadão: alguns aspectos da jurisprudência do STF". Nomos. Revista do Programa de Pós-Graduação em Direito da UFC. V. 1-1978-Fortaleza, Edições Universidade Federal do Ceará, n. semestral. Órgão oficial do Programa de PósGraduação em Direito da Universidade Federal do Ceará.

HABERMAS, Jürgen. A inclusão do outro: Estudos de teoria política. Edições Loyola. São Paulo. 2004.

_____.Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa. Tradução: Flávio R. Kothe. Rio de Janeiro: Tempo Brasileiro, 2003.

HARARI, Yuval Noah. Homo Deus: História breve do amanhã, Editora: Elsinore, Lisboa, 2017.

Https://Www.Parliament.Uk/Business/Committees/Committees-A-Z/Commons-Select/Culture-Media-And-Sport-Committee/Inquiries/Parliament-2015/Inquiry2/ Acesso em 10.12.2018

Https://www.bbc.Com/Portuguese/Brasil-38275572. Acesso em 12.12.2018

Https://Noticias.Uol.Com.Br/Politica/Eleicoes/2018/Noticias/2018/07/24/Manipulacao-Do-Eleitor-Dispensa-Fake-News-Diz-Advogado-Eleitoral.Htm Acesso em 10.12.2018

Https://www.Cartacapital.Com.Br/Opiniao/O-Efeito-Da-Midia-Nas-Eleicoes/. Acesso em 15.12.2018

Https://Observador.Pt/2018/09/28/Ataque-Informatico-Ao-Facebook-Expos-50-Milhoes-De-Contas/ Acesso em 13.12.2018

Https://www.Dci.Com.Br/Servicos/Novos-Vazamentos-De-Dados-Pessoais-Evidenciam-Buraco-Na-Fiscalizac-O-1.737545 Acesso em 11.12.2018

PATEMAN, Carole. Participação e teorias da democracia. Tradução de Luiz Paulo Rouanet. Rio de Janeiro: Paz e terra, 1992.

PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

SCHUMPETER, Joshep. Capitalismo, Socialismo e Democracia. Editado por George Allen e Unwin Ltd., traduzido por Ruy Jungmann. — Rio de Janeiro: Editora Fundo de Cultura, 1961.

SILVEIRA, Alessandra; ABREU, Joana; FROUFE, Pedro; FERNANDES, Sophie Perez; "A reforma do regime de proteção de dados pessoais e a sua implementação no ordenamento jurídico português", in E-book do IV Seminário Internacional Hispano-Luso-Brasileiro sobre Direitos Fundamentais e Políticas Públicas. Corunha, 2018.

ZAGREBELSKY, Gustavo. Il diritto mi- te. Leggi, diritti, giustizia, Einaudi,. Torino 1992.