

Governança algorítmica e a tutela do direito fundamental aos dados pessoais no Brasil: A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) como sistema protetivo para a efetivação da governança dos dados particulares nas redes sociais¹

Ana Karoline Fernandes de Sousa

Aluna do 4º período do curso de Direito da UNDB.

Raquel Colins Andrade

Aluna do 4º período do curso de Direito da UNDB.

Julia Barros de Brito

Aluna do 4º período do curso de Direito da UNDB.

Resumo: Um dos mecanismos utilizados na internet é o uso de algoritmos, que são basicamente uma sequência lógica de raciocínios que usam a coleta de dados para chegar a um resultado final de forma precisa. São eles, por exemplo, que mostram um anúncio certo sobre um produto que o internauta está desejando, ou dão dicas sobre onde achar determinada coisa de necessidade do usuário, baseado no seu comportamento prévio. Tal funcionalidade pode ser útil e facilitar o frenesi da vida moderna, como também pode ser perigosa e usar essa coleta de dados para um fim ilícito, ou que não seja da vontade do titular desses dados. Há uma linha tênue entre essas duas situações, ilustrando o problema a ser discutido nesse trabalho, visto que a legislação brasileira que trata dessas situações é demasiada recente, como a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018). Tendo em vista a importância dos direitos fundamentais, em especial o da privacidade e à informação, o presente trabalho visa a discutir o uso de algoritmos na internet e como eles estão presentes na vida dos usuários desse meio tecnológico. Para isso, foi utilizada pesquisa bibliográfica, dedutiva, além das previsões legais acerca desse mecanismo.

Palavras-chave: Governança algorítmica. Redes sociais. Privacidade. Direitos fundamentais.

Sumário: **1** Introdução – **2** A governança algorítmica e a proteção de dados pessoais – **3** Os dados pessoais conforme a LGPD (Lei nº 13.709/2018) – **4** O impacto da Lei Geral da Proteção de Dados Pessoais sobre as comunicações nas redes sociais – **5** Conclusão – Referências.

¹ *Paper* apresentado à disciplina de Direitos Fundamentais na Unidade de Ensino Superior Dom Bosco (UNDB).

1 Introdução

Hodiernamente, observam-se na sociedade atual diversas falhas no tocante às redes sociais, principalmente quanto à proteção de dados de usuários. Em relação a esse assunto, tais dados merecem a devida proteção, que tem como base o preceito constitucional da privacidade previsto no art. 5º, inciso X, da Constituição Federal (BRASIL, 1988).

Dessa maneira, cabe mencionar a existência da Lei nº 13.709/2018, que se encontra em *vacatio legis*. Por isso, serão analisadas neste trabalho as aplicabilidades da LGPD e se ela promove, em seu texto, a concretização do direito fundamental à privacidade, ou se será efetiva após o período de vacância. Além disso, será explicada a expressão “governança algorítmica”, que é ainda pouco explorada no cenário jurídico pátrio. Nesse caso, “algoritmo é um processo sistemático para a resolução de um problema” e precisa ser usado corretamente, por isso o termo “governança” (SZWARCFITER; MARKENZON, 1994).

A proteção dos dados pessoais é evidenciada no tocante ao uso de algoritmos para a coleta de informações referentes ao uso e aproveitamento desses dados do usuário nas redes sociais. A problemática se institui diante da linha tênue que separa o uso correto desses dados pessoais que alimentam os algoritmos, os quais direcionarão *posts* e anúncios para melhorar a interatividade dos internautas, em contraposição ao uso indevido, que é o uso contrário da destinação lícita.

Assim sendo, torna-se evidente que a LGPD, recentemente aprovada no Brasil, visa à proteção desses dados e, da mesma forma, a constante vigilância acerca desses dados. Como apontado neste trabalho, sabe-se que a internet está em constante transformação e inovação. Portanto, é indubitável que a forma de controle deve seguir essas transformações, com o intuito de tornar a proteção desses dados eficaz.

Outrossim, será tratada, aqui, a relação entre o usuário de redes sociais e os programadores destas, relação que será regulamentada pela LGPD, quando entrar em vigor. Este tópico é de suma importância, pois há uma lacuna legislativa acerca das relações cibernéticas, principalmente entre criador e usuário do meio utilizado.

Nesse viés, utilizou-se pesquisa bibliográfica, qualitativa, sendo um estudo descritivo realizado por meio de pesquisa bibliográfica em livros, artigos, periódicos, *sites*, anais constitucionais, entre outros. Para isso, foram pesquisados registros bibliográficos, textos legislativos, bem como as redações da Lei nº

13.709/2018. O estudo bibliográfico selecionou as principais partes que fundamentam este trabalho, além de ter seu conteúdo analisado e utilizado como fundamentação para a análise da lei e sua possível efetividade na seara da proteção de dados sensíveis e pessoais dos usuários de redes sociais.

2 A governança algorítmica e a proteção de dados pessoais

A expressão “governança algorítmica” ainda é prematura no Brasil, tendo mais enfoque no campo de sistemas de informações ou economia; no entanto, ela não se limita a esses cenários, também sendo importante no âmbito jurídico, pois é nessa seara que se dará a tutela da proteção dos dados pessoais utilizados pelos algoritmos.

Sobre os conceitos de algoritmos, governança algorítmica e como esta pode ajudar na proteção dos dados pessoais do internauta, Wemann (2018) dispõe brilhantemente em sua tese monográfica acerca do que significam e como funcionam no ordenamento brasileiro. A autora, inclusive, fala da carência legislativa brasileira a respeito do tema, um problema que, teoricamente, foi sanado com a LGPD, contemporânea à publicação de seu trabalho.

Tendo em vista o que foi dito, Wemann (2018, p. 41 *apud* BUTTERFIELD, 2016) inicia sua exposição conceituando algoritmos como “um conjunto previsto de regras ou instruções bem definidas para a solução de um problema, como o desempenho de um cálculo, em um número finito de etapas”. Diante disso, há uma primeira concepção de que esses algoritmos seriam utilizados tão somente para a área da informática, mas, como esclarece Wemann (2018), sabe-se que sua utilização pode ser feita em outros ramos.

Tem-se a noção de que esse conjunto de regras é matemático, objetivo e neutro. Entretanto, Wemann (2018) afirma que, devido à falta de neutralidade desses algoritmos, vem sendo crescente a discriminação e o controle social. Assim sendo, o controle social evidenciado em sua tese monográfica ressalta os riscos do uso inadequado dos algoritmos na sociedade, que hoje é afirmada como *capitalismo de vigilância* (WEMANN, 2018). Sabe-se que a proteção dos dados pessoais diante do emprego de algoritmos fica sujeita à ética e ao respeito às legislações vigentes. Contudo, é notório que ocorrem violações, como acontece na utilização de *Big Data*, que Wemann (2018) clarifica como coleta e análise.

Seguindo o exposto por Mattiuzzo (2019), a ascensão da *Big Data* acentuou a utilização de algoritmos, e essa relação não ocorre aleatoriamente. Sabe-se,

como evidenciado acima o conceito de algoritmos, que *Big Data* pode ser conceituada como uma compilação de informações de diferentes fontes. Essas informações são processadas, gerando um banco de dados, devendo ser destacado que, dentre esse compilado de informações, estão os dados pessoais (MATTIUZZO, 2019).

Isto posto, faz-se necessário entender como a proteção dos dados pessoais está atrelada à governança algorítmica. À vista disso, Corrêa e Gediel (2008) discorrem sobre a proteção jurídica dos dados pessoais, dando um enfoque histórico mundial, falando de clássicos distópicos como *1984*, de George Orwell, e *Admirável Mundo Novo*, de Aldous Huxley, e como o cenário da troca constante de informações se tornou o que é hoje. Em que pese a complexidade das relações sociais e o crescente fluxo de dados pessoais, devido ao desenvolvimento tecnológico, Corrêa e Gediel (2008) dispõem que a proteção do titular desses dados ocorre tanto em relação ao acesso, como ao seu tratamento, utilização e circulação.

É indubitável que o controle do fluxo de informações relacionado aos dados pessoais tem o escopo de assegurar a igualdade de tratamento dos cidadãos, respeitando sua intimidade. A disposição de informações ligadas ao que se consideram dados pessoais de uma pessoa identificada ou identificável é pontuada como:

Nome, o endereço, o telefone, os números dos documentos de identificação, mas também currículos escolares, dados profissionais, fiscais e bancários, dívidas e créditos, meios de pagamento, o endereço eletrônico, o IP (Internet Protocol – que permite a identificação do usuário de computador), imagens recolhidas por câmeras de segurança, fotografias disponibilizadas na Internet, e, ainda, hábitos de consumo, dados de saúde e biométricos (CORREA; GEDIEL, 2008, p. 144).

Dessarte, percebe-se como o controle acerca dos referidos dados pessoais influencia no controle social. À vista disso, Corrêa e Gediel (2008) explicam como a demanda de informações relativas à intimidade dos cidadãos e consumidores é estabelecida por meio da tecnologia e dos meios de comunicação pelo que se chama de *sociedade de controle*. Em suma, seguindo o exposto pelos autores supracitados, a *sociedade de controle* é caracterizada pelo controle de dados referentes ao acesso de informação das massas e não somente de um indivíduo isolado.

Assim, sobre a demanda de informações relativas à intimidade dos usuários de redes sociais, há de se reconhecer que o indivíduo é livre para postar o que quiser – dentro das diretrizes do *site* acessado – mas o programador do *site* não pode dispor desse conteúdo de forma livre sem consentimento do usuário. Acerca do consentimento, discorre José Gomes Canotilho (2018):

Afirmar que o ser humano é livre exige, não como seu pressuposto, mas como consectário, reconhecer seu domínio ou controle sobre os inputs e outputs de informação. O direito à intimidade está mais associado ao controle de outputs informacionais, desde a sua obtenção por outros até seu uso ulterior. Diz-se assim que o direito à intimidade concede um poder ao indivíduo para controlar a circulação de informações a seu respeito. As informações que se encontram protegidas são aquelas de caráter “privado”, “particular” ou “pessoal”. É o mesmo que dizer, ainda que sob os riscos da tautologia, aquelas informações associadas às particulares do ser. Na caracterização da “informação pessoal” se deve ter em conta: o papel da vontade, a definição do que seja “obtenção de informação”, a compreensão do termo “uso de informação” e a natureza ampla de informação “pessoal” (CANOTILHO, 2018, p. 292-293).

Depreende-se, do título desta seção, certa dicotomia entre as expressões “governança algorítmica” e “proteção de dados pessoais”, pois, de fato, há certa incompatibilidade entre as duas se não forem aplicadas corretamente. O que não é estranho no âmbito constitucional, pois normas constitucionais ou direitos fundamentais entram constantemente em conflito quando utilizados no plano concreto. Por isso, há de se ponderar quais princípios devem ou não prevalecer no caso prático, o que é decerto complicado, já que as formas clássicas para solução de antinomias (critério hierárquico, temporal e especial) são insuficientes no plano constitucional (SARMENTO, 2017).

Nesse sentido, o constitucionalista Daniel Sarmiento (2017) explica que não há hierarquização das normas constitucionais, assim, o direito à informação (art. 5º, XIV, CF/88) é tão importante quanto o direito à privacidade. A sua solução para o problema, não tão diferente é da exposta por Mendes e Franco (2014), ao falarem dos pesos dos direitos fundamentais quando usados no caso concreto, em que o direito considerado mais relevante ao caso terá maior peso e, assim, preferência de aplicação.

Portanto, Sarmento (2017) fala da possibilidade do critério hierárquico para a solução de antinomias constitucionais, no sentido de que não haverá uma hierarquização de direitos, mas sim uma preferência de direito a ser tutelado no caso em pauta. Prossegue dizendo que “nessa hipótese, não se teria a invalidação da norma reputada inferior, com sua exclusão do ordenamento, mas tão somente a sua não aplicação na hipótese de conflito” (SARMENTO, 2017). Assim, é possível concluir que a governança algorítmica é justamente o uso adequado dos algoritmos para coletar informações importantes, que serão usadas para melhorar a interação do usuário de redes sociais com as propagandas ou assuntos que lhes são apresentados, sem, contudo, invadir seu espaço privado.

3 Os dados pessoais conforme a LGPD (Lei nº 13.709/2018)

A Lei Geral de Proteção de Dados parte de uma discussão que Rodotá (2008) disserta que não é apenas a mera fortificação da esfera privada contra invasões externas, como também o arcabouço de informações é um componente da organização de poder, ou seja, algum grupo ou indivíduo dirige o exercício do poder conforme a viabilização dos dados pessoais, em que há a necessidade de simplificar a alteração entre liberdades individuais e eficiência administrativa e empresarial para modos contra o controle. Análogo à ilustração de George Orwell na obra *1984*, que retrata o futuro autoritário de um Estado pós-guerra e a figura do “grande irmão” que edita a verdade e há a perda total de identidade do sujeito, resultando no debate em torno da falta de neutralidade na era tecnológica, a legislação em questão e se existe limite na regulação da liberdade em detrimento de outros direitos.

Logo, pela própria natureza de massificação de conteúdo em milissegundos através da internet, o compartilhamento um tanto irracional de todos os pequenos atos diários através das redes sociais e a ingenuidade no fornecimento de informações. Algo que colabora para uma falsa sensação de segurança da sociedade, em que não há preocupação com o cenário atual, em que os dados pessoais são utilizados rotineiramente como “moeda de troca” para a comercialização de empresas (GOMES; BITTENCOURT, 2019). Portanto, é perceptível a necessidade de proteção de dados pessoais na medida que casos tão repercutidos, como o vazamento de dados do Facebook, enfatizam a necessidade da maior autonomia na proteção de dados.

Antes da cominação legal da Lei nº 13709/2018, o assunto já era comentado no plano internacional como o direito de *privacy* norte-americano, que, embora empregue esse nome, trata-se da vedação da intimidade (RUARO; RODRIGUEZ, 2010). No entanto, a indispensabilidade da legislação brasileira se espelhou na autodeterminação informacional europeia, no tocante ao Regulamento Geral sobre a Proteção de Dados (GDPR), que entrou em vigor em maio de 2018, concernente ao escândalo de coleta de dados mundiais pela National Security Agency norte-americana exposta por Edward Snowden. Por conta disso, as noções passaram a mostrar maior cautela com suas leis de defesa de dados (GOMES; BITTENCOURT, 2019).

Conforme Gediel e Côrrea (2008), o direito de proteção de dados pessoais refere-se à proteção da intimidade, como consta no art. 5º, X, da CF/88, e no art. 21 do CC/2002, assim como o direito à informação, incluso no art. 5º, XVI, da CF/88. Sobre os direitos fundamentais, Mendes e Branco (2014) abordam quais são e suas características, bem como se dá a tutela acerca desses direitos pautados no catálogo da CF/88. Ou seja, a LGPD visa a blindar o que, de certo modo, já é incluso no ordenamento jurídico, apenas complementando as entrelinhas que o Marco Civil da Internet não preenchia, em que “A LGPD complementa, harmoniza e unifica um ecossistema de mais de quarenta normas setoriais que regulam, de forma direta e indireta, a proteção da privacidade e dos dados pessoais no Brasil” (MONTEIRO, 2018, p. 9).

Ademais, a Lei Geral da Proteção de Dados Pessoais, além de regular o tratamento de dados por pessoa jurídica ou natural, resguarda os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade natural. Há uma série de pontos-chave na legislação, como os fundamentos de fortalecimento tutelar dos direitos análogos ao arcabouço informacional dispostos no art. 2º, tal como a finalidade dos direitos humanos dissertado no mesmo artigo (MULHOLLAND, 2018).

Considera-se os diferentes setores que se estruturam pelo uso de dados pessoais como método de oferta dos seus serviços para que o *marketing* direcionado seja de fato efetivo, ponderando pela lei a frágil posição à qual aqueles localizados nas redes da *web* estão suscetíveis. Por isso, inclui-se medidas de regramento da disponibilização de informação para que se evitem práticas abusivas, havendo a adequação do escudo de utilização informacional pela previsão de novos direitos positivados no art. 5º da LGPD (MONTEIRO, 2018).

Mantendo a linha de raciocínio que a lei resguarda ao tratamento de dados pessoais, descrito pelo art.5º, X 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; (BRASIL, 2018).

Evidentemente, mencionando o catálogo descritivo das atividades acerca dos dados pessoais que serão regulamentadas pela lei, é de extrema pertinência comentar que a lei passa a requerer a manifestação da vontade expressa em torno de qualquer tratamento de informação pessoal (GOMES; BITTENCOURT, 2019). Ou seja, deve haver o consentimento dos termos de uso de qualquer rede social, sendo este o requisito que possibilita o controle do indivíduo para que o agrupamento de seus dados encontra-se vedado por lei. Porém, surge uma lacuna pela própria natureza veloz das relações nas redes sociais: o consentimento é agrupado dentro das políticas de privacidade e somente com sua concordância pode ser usado o serviço ofertado, em outras palavras, as políticas de uso e privacidade são conjuntas.

Entretanto, nota-se que o consentimento é usado apenas para dar valor a tais modelos de negócios e não para proteger os dados em si. Esse mecanismo é falho, uma vez que não permite que o usuário goze de sua autodeterminação informativa, pois cabe apenas a ele aceitar ou recusar o serviço utilizado (GOMES; BITTENCOURT, 2019, p. 30).

No momento em que o legislador inclui o consentimento como um dos pontos principais, uma série de princípios podem ser observados, sobre os quais Monteiro (2018) diz que a vontade expressa do indivíduo complementa o princípio da transparência, abordando o direito à transparência que a lei abrange, portanto, o direito de obter informações claras e acessíveis, o que também é visto nas leis europeias que discutem o mesmo tema. Assim como o direito de acesso aos dados, que assim como o direito à transparência consta no artigo 19:

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato

simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular (BRASIL, 2018).

Relembra-se Rodotá, supracitado, que é necessária uma tutela rígida e exigente quando se trata de dados sensíveis pela priorização da isonomia da sociedade. Logo, as liberdades individuais são fortalecidas pelo papel que LGPD se propõe a cumprir; no entanto a legislação brasileira ainda peca em torno do consentimento, que não é explícito contraposto a legislações europeias. Em suma, é visível que há vitalidade na proteção de dados pessoais pelo exercício regular de direitos fundamentais, assim como o não controle sucessivo.

4 O impacto da Lei Geral da Proteção de Dados Pessoais sobre as comunicações nas redes sociais

Danilo Doneda (2011) aborda o tema do desenvolvimento das leis de proteção de dados no contexto internacional e brasileiro, sendo interessante o fato de que seu artigo, datado de 2011, isto é, anterior ao Marco Civil da Internet e à LGPD, já trazia a discussão da necessidade de uma proteção legislativa sobre os dados pessoais, principalmente no campo cibernético. A análise de outro artigo de Doneda (2016) também propiciou a conclusão de que, quando se trata dessa seara do direito, há uma necessidade de atualização constante, visto a volatilidade das relações e inovações que a internet acarreta. O que, no entanto, não deve significar uma insegurança jurídica, pois é função do legislador e dos juristas a garantia de meios que tutelem os direitos supracitados.

Nesse viés, a LGPD (Lei nº 13.709/2018) trata-se de uma evolução no direito brasileiro, pois aborda incisivamente temas cibernéticos – campo ainda pouco explorado no âmbito jurídico – e as normas explicativas que nela constam, como o art. 5º, I, que define dado pessoal como “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018). Quando aplicada às redes sociais, em que basicamente tudo é dado pessoal – já que a exposição dos usuários é tamanha que chega a ser possível descobrir muito sobre a vida do sujeito, sem muito esforço –, a lei torna-se de suma importância, pois passará a reger a relação entre usuário e programador, baseada no direito à explicação (MONTEIRO, 2018).

Nesse viés, Pablo Monteiro (2018) trata do direito à explicação, que diz respeito a um direito do indivíduo, que tem suas informações coletadas, de saber como se dá essa coleta, quem a fez e o que fará com os dados retidos. Esse direito é uma derivação do princípio da transparência, que já existia no ordenamento brasileiro, mas só se tornou capaz de tutelar amplamente os casos relacionados ao universo cibernético após a ratificação da LGPD. O autor pontua que o maior impacto da lei – no caso sobre as comunicações nas redes sociais – foi a instauração de princípios gerais contidos no texto normativo.

Destaca-se, assim, um princípio importante na seara das redes sociais: o da transparência. Segundo o autor, o princípio da transparência “deve reger toda e qualquer relação do responsável pelo tratamento de dados pessoais com o titular dos dados, garantindo a este o direito de acesso aos seus dados pessoais” (MONTEIRO, 2018, p. 10). Também institui o pressuposto do dever à informação acerca dos critérios de tratamentos que receberão os dados, onde e com qual fim serão aplicados (MONTEIRO, 2018).

Sobre a expressão “transparência algorítmica”, Lauren Smith (2016) ressalta a dificuldade que as companhias têm para seguir esse padrão. Pois, geralmente quando elas liberam informações sobre como funcionam os seus sistemas de coleta de dados, os usuários não entendem nem mesmo o significado de algoritmo, tornando difícil essa comunicação entre o indivíduo que usa a rede social e o que coordena o *site*. Um exemplo comum disso são os termos de uso, exibidos antes de o indivíduo criar sua conta em uma rede social. Lá estão todas as regras e diretrizes que ele tem que seguir e as quais ele permite que a empresa siga, como coletar dados para melhorar a experiência e utilizá-los quando quiser.

A autora supracitada usa os EUA como exemplo, e ressalta a carência de leis que tratem sobre o assunto, o que já não é um problema no Brasil, pois a LGPD aborda justamente essa problemática. No entanto, como Smith (2016) ressalta, os usuários norte-americanos não leem os termos de uso, tampouco os brasileiros; dessa forma, as companhias de redes sociais, para operarem no Brasil, têm que seguir a legislação local, mas podem definir suas diretrizes na preferência que optarem, contanto que peçam permissão ao usuário. Este, como de praxe, permite sem ao menos ler o que está fazendo, ao passo que a automatização dos *sites* é incrementada constantemente. Por isso, os usuários “vão ficando cada vez menos capazes de compreender, explicar ou prever o funcionamento interno, os vieses e os eventuais problemas dos algoritmos” (DONEDA, 2016, [n.p.]).

Destarte, Mulholland (2018) afirma que a utilização de dados sensíveis é um problema recorrente que causa sérios danos à privacidade dos cidadãos que têm suas informações violadas. A autora narrou casos de roubos e uso indevido de dados que ocorreram em outros países, mas há impactos no Brasil, devido ao cosmopolitismo proporcionado pelas redes sociais; por isso, ressalta a importância e a efetividade da LGPD na tutela desses direitos.

Por fim, os autores que já pautaram sobre o tema da governança algorítmica ressaltam a importância de uma estrutura normativa estatal, que regule ou mesmo limite o uso dos algoritmos. Contudo, é um tema de profunda complexidade e de pouco enfoque legislativo, não sendo exequível ou eficaz um texto normativo que trate apenas disso (MACHADO, 2018). Dessa forma, a LGPD já proporciona diretrizes adequadas para a proteção de dados pessoais quando se trata de redes sociais, principalmente no respeito à privacidade e ao direito à explicação. Assim, quando entrar em vigor, é de se esperar um impacto positivo da lei sobre as comunicações nesse âmbito.

5 Conclusão

Ao longo do presente trabalho, buscou-se analisar a governança algorítmica na internet, seus sinais de existência no cotidiano virtual e sua intersecção na esfera jurídica através da vedação dos dados pessoais. Essa falta de neutralidade na rede verifica uma forma de constante vigilância e controle sem qualquer critério ético ou consentimento. Por isso, ficou clara a necessidade da promulgação de uma legislação que tutele as informações dos internautas. Dessa forma, a Lei Geral de Proteção de Dados Pessoais tem o intuito de agir como um filtro do banco de dados devido à movimentação constante de conteúdo, ou seja, para tal investigação foram usadas leis estrangeiras como parâmetro de impacto do que a LGPD poderá vir a cumprir.

Em virtude dos fatos mencionados, a lei supracitada protegerá o que, de forma um tanto implícita, no ordenamento jurídico; logo, preenche lacunas deixadas pelo Marco Civil da Internet ao tecer um arcabouço harmônico de resguardo de dados pessoais. Ainda que prematuro na legislação, o tema é discutido pertinentemente e avidamente antes mesmo da cominação da Lei 12.695/2014, como foi dito anteriormente, evidenciando o desenvolvimento do direito acerca do assunto.

Entretanto, ficou evidente que há um problema quanto a um dos pontos fulcrais da LGPD, que se baseia na ideia de consentimento quando se trata do

compartilhamento de dados, frisando principalmente o *marketing* direcionado, uma vez que a manifestação de vontade para a permissão do acesso à informações é, até certo ponto, sorrateira. Ou seja, quando se discute a própria natureza veloz da *internet*, não há uma lógica cautelosa dos internautas para o acesso de certos *sites* e aplicativos, em outras palavras, o consentimento é fornecido livre de qualquer compreensão ou sequer consciência do internauta. Versando sobre esse tema, é intrínseca a compreensão da transparência na LGPD, que o usuário deve ser explicado, de forma clara e direta, de quando e como seus dados vão ser acessados e conseqüentemente, armazenados, algo que GDPR (Lei Regulamento Geral sobre a Proteção de Dados) disserta mais fervorosamente.

Destarte, a notoriedade da LGPD como artifício essencial para o uso da rede e garantia dos direitos dos indivíduos que a utilizam foi exposta, em que os escândalos do mau uso de dados pessoais possuíram um grande papel na observação do caráter indispensável da lei em questão. Por conseqüência, a Lei Geral de Proteção de Dados é uma medida devida, todavia não suficiente uma vez que, segundo exposto anteriormente, há certos obstáculos no quesito consensual assim como o enraizamento da ideia de informações pessoais como tesouro pela indústria.

Algorithmic governance and data protection as a fundamental right in Brazil: The General Data Protection Act (LGPD) as a protection system for the effective governance of private data on social media

Abstract: One of the mechanisms used on the internet is the use of algorithms, which are basically a logical sequence of reasoning that uses data collection to arrive at a final result in a precise way. They show, for example, a certain ad about a product that the user is looking for, or give tips on where to find a certain thing that the user needs, based on their previous behavior. Such functionality can be useful and facilitate the frenzy of modern life, but it can also be dangerous and use this data collection for an illicit purpose, or that is not the will of the data subject. There is a fine line between these two situations, illustrating the problem to be discussed in this work, since the Brazilian legislation that deals with these situations is too recent, such as the General Data Protection Law (LGPD - Law 13.709/2018). In view of the importance of fundamental rights, especially privacy and information, this paper aims to discuss the use of algorithms on the internet and how they are present in the lives of users of this technological environment. For this, bibliographic research was used, deductive in addition to the legal provisions about this mechanism.

Keywords: Algorithmic governance. Social networks. Privacy. Fundamental rights.

Referências

- BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*, 1988. Brasília: Senado Federal, Centro Gráfico, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 4 jul. 2020.
- BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 ago. 2019.
- CANOTILHO, J. J. Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lenio Luiz (Coord. científica). *Comentários à Constituição do Brasil*. 2. ed. São Paulo: Saraiva, 2018.
- CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção Jurídica de dados pessoais: a intimidade sitiada entre o Estado e o Mercado. *Revista da Faculdade de Direito UFPR*, Curitiba, n. 47, p. 141-153, 2008.
- DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law*, v. 12, n. 2, p. 91-108, 2011.
- DONEDA, Danilo; ALMEIDA; Vírgilio A. F. O que é governança de algoritmos? *Politics: uma publicação Nupef*, Rio de Janeiro, 2016. Disponível em: <https://politics.org.br/edicoes/o-que-%C3%A9-governan%C3%A7a-de-algoritmos>. Acesso: 31 out. 2019.
- GOMES, Évelyn Vieira; BITTENCOURT, Izabella Alves Jorge. O consentimento nas leis de proteção de dados pessoais: análise do regulamento geral sobre a proteção de dados europeu e da lei brasileira 13.790/2018. In: POLIDO, Fabricio; ANJOS, Lucas; BRANDÃO, Luiza (Orgs.). *Políticas, internet e sociedade*. Belo Horizonte: IRIS, 2019. p. 26-35. Disponível em: https://www.academia.edu/39853391/O_LIVRE_DESENVOLVIMENTO_DA_IDENTIDADE_PESSOAL_EM_MEIO_DIGITAL_PARA_AL%3%89M_DA_PROTE%3%87%3%83O_DA_PRIVACIDADE?auto=download. Acesso em: 4 jul. 2020.
- MACHADO, H. F. de S. Algoritmos, regulação e governança: uma revisão de literatura. *Revista de Direito Setorial e Regulatório*, Brasília, v. 4, n. 1, p. 39-62, maio 2018. Disponível em: <http://periodicos.unb.br/index.php/rdsr/article/view/19131/17671>. Acesso em: 02 out. 2019.
- MATTIUZZO, Marcela. Algorithms and Big Data: considerations on algorithmic governance and its consequences for antitrust analysis. *Revista de Economia Contemporânea*, v. 23, n. 2, p. 1-19, 2019. Disponível em: <http://www.scielo.br/pdf/rec/v23n2/1980-5527-rec-23-02-e192328.pdf>. Acesso em: 30 set. 2019.
- MENDES, Gilmar F.; BRANCO, Paulo G. G. *Curso de Direito Constitucional*. 9. ed. São Paulo: Saraiva, 2014.
- MONTEIRO, R. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? *Instituto Igarapé*, Artigo Estratégico 39. Rio de Janeiro, dez. 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 04 jul. 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *R. Dir. Gar. Fund., Vitória*. v. 19, n. 3, p. 159-180, 2018.

RODOTÁ, Stefano. *A vida na sociedade de vigilância: privacidade hoje*. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. *Revista Direito, Estado e Sociedade*, n. 36, 2010. Disponível em: <https://revistades.jur.puc-rio.br/index.php/revistades/article/view/212>. Acesso em: 02 set. 2019.

SARMENTO, Daniel. *Direito Constitucional: Teoria, História e Métodos de trabalho*. 2. ed. Belo Horizonte: Fórum, 2017.

SMITH, Lauren. Algorithmic transparency: Examining from within and without. *IAPP Privacy Perspectives*, 2016. Disponível em: <https://iapp.org/news/a/algorithmic-transparency-examining-from-withinand-without/>. Acesso em: 02 out. 2019.

SZWARCFITER, J. L.; MARKENZON, L. *Estruturas de dados e seus algoritmos*. Rio de Janeiro: Livros Técnicos e Científicos, 1994.

WEMANN, Larissa. *Governança algorítmica e a proteção de dados pessoais*. Orientador: Fabiano Menke. 2018. 77 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Jurídicas e Sociais) – Curso de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: <https://www.lume.ufrgs.br/bitstream/handle/10183/174601/001061235.pdf?sequence=1>. Acesso em: 29 ago. 2019.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

SOUSA, Ana Karoline Fernandes de; ANDRADE, Raquel Colins; BRITO, Julia Barros de. Governança algorítmica e a tutela do direito fundamental aos dados pessoais no Brasil: A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) como sistema protetivo para a efetivação da governança dos dados particulares nas redes sociais. *Revista Fórum de Direito na Economia Digital – RFDED*, Belo Horizonte, ano 4, n. 6, p. 9-22, jan./jun. 2020.
