

RESPONSABILIDADE NA INTERNET: OS PERIGOS DO *BIG DATA* PARA A PRIVACIDADE

RESPONSIBILITY ON THE INTERNET: THE DANGERS OF BIG DATA FOR PRIVACY

Victor Werneck Gomes¹

RESUMO

O presente artigo pretende adentrar na área do Direito Digital, estritamente para demonstrar uma das diversas inovações na área do direito, especificamente na relação entre a tecnologia e a privacidade no restrito tema do *Big Data*, termo que pode-se relacionar a mineração de dados e coleta daquilo que os usuários desempenham nas redes de internet. A necessidade atual que o presente objeto de estudo procura investigar é de se discutir se os limites da mineração de dados na atualidade são suficientes e se existe necessidade de mudança no legislativo brasileiro. Atualmente já existem certas leis no Brasil para tratar sobre a proteção da privacidade em mineração de dados, bem como outras situações relacionadas a movimentação destes dados, o que poderia abrir caminho para outras mudanças no ordenamento jurídico, especificamente sobre o *Big Data*. Ocorrerá a explicação de algumas temáticas do Direito relacionado a tecnologia, *Big Data* e também sobre o recaimento do tema no Direito do Consumidor, e após estas explicações, qual a situação atual do tema no Brasil e se discutirá a possível aplicação para a proteção da privacidade.

Palavras-chave: *Big Data*, Privacidade, Internet, Direito do Consumidor, Direito Digital.

ABSTRACT

This article intends to enter the area of Digital Law, strictly to demonstrate one of the several innovations in the area of law, specifically in the relationship between technology and privacy in the restricted theme of Big Data, a term that can be related to data mining and collecting what users perform on internet networks. The current need that the present object of study seeks to investigate is to discuss whether the limits of data mining today are sufficient and whether there is a need for change in the Brazilian legislature. Currently, there are already certain laws in Brazil to deal with the protection of privacy in data mining, as well as other situations related to the movement of this data, which could pave the way for other changes in the legal system, specifically on Big Data. There will be an explanation of some thematic of Law related to technology, Big Data and also about the relapse of the theme in Consumer Law, and after these explanations, what is the current situation of the theme in Brazil and the possible application for the protection of privacy will be discussed.

Keywords: Big Data, Privacy, Internet, Consumer Law, Digital Law.

¹ Advogado - OAB/MG, Mestrando em Direito - Universidade FUMEC; Especialista em Direito Público – PUCMINAS; Especialista em Direito Processual Civil - Universidade Cândido Mendes; Bacharel em Direito - PUCMINAS

1 INTRODUÇÃO

O tema em questão ressurgiu para um recorrente conflito no Direito da atualidade, a relação que necessita de ser sempre equilibrada entre as esferas da informação e da privacidade.

De fato, sobre a mineração de dados, talvez estejamos diante da maior questão atinente a internet das últimas décadas. Porém, a problemática surge a partir do ponto de que a tecnologia vem avançando em determinada escala que já não consegue ser acompanhada pelas legislações brasileiras ou pelo mundo jurídico.

Para tentar acompanhar os avanços tecnológicos, surgiu a recente Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), que em geral é um avanço para o tema, porém em diversos pontos ela já se tornou defasada ou se falta pouco para outros pontos estarem em atraso, e a coleta de dados em massa diz respeito justamente a esta legislação.

A coleta de dados em massa diz respeito a uma realidade na qual se pode reparar em diversos momentos na utilização da internet, pois ela ocorre a todo momento.

Um exemplo para tal, é quando se utiliza as redes sociais, pelo fato de que tudo aquilo no qual pesquisamos em uma outra plataforma é coletado, ou seja, quando um usuário estiver pesquisando um determinado produto de certa marca, quando este usuário retornar a rede social teremos propagandas destes produtos para que o mesmo seduza o consumidor a adquiri-lo.

Desta forma, se faz necessário discutir os limites em que a informação do usuário pode ser disponibilizada para terceiros. Obviamente, a discussão não engloba a atuação da ferramenta em situações onde não há violação de privacidade, como em coleta de outros tipos de informação e dados.

Sendo assim, a ferramenta não atingiria a violação a privacidade quando se relaciona a seus usuários ou consumidores? Não haveria a necessidade de maior limitação na utilização do *Big Data* e outras ferramentas de inovação para coibir o acesso a dados dos usuários?

2 BIG DATA

O termo *Big Data*, do sentido da palavra, significa o alto volume de processamento de dados, a mineração dos dados existentes na internet. Esta coleta ou mineração de dados feita no uso da internet, em todos os usuários, tal qual pode ser conceituado por Gunther²:

Big Data pode ser definido com base em grandes volumes de dados amplamente variados que são gerados, capturados e processados em alta velocidade. Como tal, esses dados são difíceis de processar usando as tecnologias existentes. Ao adotar tecnologias analíticas avançadas, as organizações podem usar big data para desenvolver insights, produtos e serviços inovadores.

Sendo assim, trata-se grande volumes de dados que são extremamente avançados mesmo se olhar para uma ótica de uma década atrás. Com o uso atualmente, a ferramenta se torna algo extremamente operante para serviços de inovação.

Patrícia Peck Pinheiro³, também aborda o tema do *Big Data*, demonstrando como ele é visto no momento:

O assunto do momento das empresas da era digital, mais sustentável, cujas ações valem mais na Bolsa, é o “big data”. Ou seja, como gerar negócios com o grande banco de dados global que se tornou a web, principalmente com todas as informações publicadas pelas próprias pessoas na era pós-web 2.0. Quanto maior o potencial, maior o valor da própria empresa. Por isso, qualquer lei sobre privacidade, proteção de dados sensíveis, para ser eficaz, tem que ser reflexo do modelo socioeconômico estabelecido e servilo. Se há discussões éticas sobre o modelo, devemos rever o próprio modelo antes de aplicar uma lei mais rígida que possa ter dois efeitos: a) não ser cumprida (dificuldade de impô-la inclusive para empresas fora do ordenamento jurídico de origem dos dados) e b) gerar como retaliação o apagão digital de protesto (as empresas retirarem os serviços do ar, o que lhes é de direito, visto que não terá mais como se pagar, pois não poderão usar os dados).

Como explicado, é de extrema importância a incidência do *Big Data*, frente a privacidade e temas correlatos. Para o mesmo, o Brasil hoje trouxe algumas legislações para tentar coibir desusos da ferramenta.

² GÜNTHER, Wendy Arianne et al. Debating big data: A literature review on realizing value from big data. *The Journal of Strategic Information Systems*, v. 26, n. 3, p. 191–209, 2017.

³ PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2013, página 43.

3 REGULAÇÃO E APLICAÇÃO NO CONTEXTO DA ATUALIDADE

Uma regulamentação existente é o Marco Civil da Internet⁴ (Lei N°12.965, de 23 de Abril de 2014), porém, o Marco Civil da Internet não trouxe suficientes informações para preencher todas as lacunas ou pelo menos a maioria delas do tema.

Patrícia Pinheiro⁵ comenta sobre as inovações vistas pelo Marco Civil da Internet, com ênfase na importância da privacidade dos dados e qual seriam as garantias com esta legislação:

A privacidade dos usuários, além de uma garantia, deve, também, ser protegida pelo Marco Civil da Internet, porque as informações dos usuários viraram moeda e são usadas como pagamento dos serviços que se dizem gratuitos, mas que retêm as informações dos indivíduos para sempre, utilizando-a para qualquer fim. Quando se fala no Marco Civil da Internet, seu propósito inicial é garantir a privacidade de dados de consumidores e ter a guarda segura dos mesmos (igualando aos demais países do exterior), complementando o texto Constitucional, o Código de Defesa do Consumidor e o Código Civil. O texto apresentado ao Congresso Nacional está bem claro quanto à garantia de liberdade de expressão, todavia, deveria ter sido tratado melhor no que diz respeito à vedação do anonimato prevista pela Constituição Federal. Além disso, privilegia o acesso à Internet a todo cidadão e deveria determinar a obrigação de o primeiro acesso ocorrer com educação sobre uso ético, seguro e legal da Internet, fazendo com que os usuários sejam conscientes, para orientá-los sobre o uso correto desta ferramenta, pois isso pode gerar abusos comuns à liberdade de expressão.

Além desta lei, também pode ser mencionado, pelo fato de relacionar a tecnologia com a área jurídica, a Lei 12.737/2012⁶, na qual surgiu com uma infelicidade da atriz Carolina Dieckmann, que sofreu uma invasão na sua privacidade no seu computador e teve arquivos pessoais subtraídos⁷.

Para tentar preencher estas lacunas, surgiu a Lei Geral de Proteção de Dados Pessoais (Lei N° 13.709, de 14 de agosto de 2018)⁸, que procurou demonstrar maiores tratativas a respeito dos dados em ambiente digital, seja estes dados de

⁴ Lei n.º 12.965, de 23 de abril de 2014. Marco Civil da Internet.

⁵ PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Saraiva, 2013, página 44.

⁶ Lei 12.737/2012, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos

⁷ JUNIOR, Eudes Quintino de Oliveira. A nova lei Carolina Dieckmann. Jusbrasil. 2012.

⁸ Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

pessoa natural ou pessoal jurídica, com o objetivo de privilegiar a privacidade, intimidade, liberdade de expressão e outros direitos, como pode ser observado em seu Artigo

A Lei Geral de Proteção de Dados Pessoais, sofreu alterações em 2019, pela Lei Nº 13.853, de 8 de julho de 2019⁹, que criou a Autoridade Nacional de Proteção de Dados (ANPD), tendo diversas funções, como segundo o Art. 55-J desta lei, dizendo a respeito de "I - zelar pela proteção dos dados pessoais...", "III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade" e "VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade". (BRASIL, 2019)

O *Big Data* utilizando-se de dados pessoais, traz a incidência da Lei Geral de Proteção de Dados, que por conseguinte traz a limitação do uso através de princípios que estão previstos no seu artigo 6º.

Em seu caput, o princípio da boa-fé, já é imediatamente abordado, onde se traz toda a carga ética, dogmática do princípio da boa fé, pois principalmente por lidar com atividades que dizem respeito aos dados de outros usuários, a boa-fé é imprescindível. Outros princípios são citados, e são extremamente relevantes, como o princípio da finalidade, afinal é extremamente necessário que os dados do usuário sejam tratados com inteira responsabilidade e que tenham objetivo explícito, quando o uso.

Sendo assim, é explicitada na Lei Geral de Proteção de Dados Pessoais¹⁰, todos os princípios, assim dispostos:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: 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;

⁹ Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

¹⁰ Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de 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;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Visto assim, que além do princípio da boa-fé e da finalidade, outros tem muita relevância constante para o Big Data, onde um preenche o outro, que é o caso do princípio da adequação e necessidade, em relação ao da finalidade.

A atuação conjunta pode ser vista, no exemplo de que alguém que recolhe dados pessoais para uma determinada finalidade, não tem permissão para buscar outros dados que não sejam aqueles referentes. Reparado assim em uma situação de que há um problema numa compra de produto, não há necessidade de outros dados pessoais do cliente além dos essenciais na utilização da ferramenta.

4 CONFLITO COM A PRIVACIDADE DO CONSUMIDOR OU DO USUÁRIO

A utilização do *Big Data* de forma indiscriminada e, principalmente, do modo em que as autorizações dos usuários são coletadas atualmente, deixa a sociedade refém de programadores e seus algoritmos. Ao mesmo tempo, essa coleta de dados deve ter regulamentação forte, mas principalmente, deve ser fiscalizada, principalmente pelas situações que podem ser encontradas na utilização da ferramenta.

Uma pratica feita pela mineração de dados, mas que não se sabe exatamente em diversos momentos em qual finalidade está sendo feita, é como o Big Data estaria atuando para personalizar ofertas e até qual limite essas informações que

são coletadas estão condicionado o próprio consumidor em adquirir x ou y produto. Como é algo incerto, é complicado prever até qual ponto a vontade do próprio consumidor acabaria por ser moldada pela publicidade desempenhada na internet. A publicidade ocorre pelo Big data, onde o consumidor, ao pesquisar determinado produto, têm para ele oferecido outras ofertas distintas, que outros consumidores tenham adquirido ou que tenham visualizado, por conta do produto anterior que fora adquirido.

Desta analogia, resta concluído que definitivamente, está sendo personalizado a forma que o consumidor navega em sites e como são demonstradas as ofertas do mesmo. Porém, até que nível pode-se chegar? Até que nível pode-se modificar a vontade de cada um sem se perceber?

As ofertas aparecem de acordo com um algoritmo, que define a partir de outros consumidores que pesquisaram e compraram o produto, onde os próximos consumidores provavelmente podem ter interesse e daí surgira para o próximo consumidor.

Isto pode ocasionar em um efeito bolha para o consumidor, que é o risco de todos ficarem presos na bolha criado pelo algoritmo que demonstra certos padrões para o consumidor, criando uma verdadeiro ciclo onde todos consomem os mesmos produtos. Como exemplos, Netflix, Spotify e YouTube. Baseado no que assistimos/ouvimos, os dados são coletados e novas sugestões nos são apresentadas, sempre dentro daquele círculo de interesses, evitando, muitas vezes, que descubramos coisas novas e ampliemos nossos horizontes.

Todas estas reflexões, esbarram na necessidade de privacidade para cada indivíduo e de acordo com os Direitos da Personalidade, premissas que estão prevista no Código Civil¹¹:

Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

¹¹ BRASIL. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002.

Da mesma forma que a privacidade também é prevista na Constituição Brasileira¹²: "Art. 5º, X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação [...]".

Resta ser visto como riscos, o fato de se pensar em até quais limites as empresas podem chegar para regular a sua publicidade para vendas, e pouco se sabe de até aonde esses dados coletados são demonstrados de forma transparente para as pessoas, o que poderia violar a privacidade de cada um.

Outro exemplo de possível violação da privacidade, que é algo natural hoje de até sites de hospedagem conseguirem definir se você pesquisou alguma cidade ou destino, utilizando-se de informações para "bombardear" os usuários de propagandas oferecendo pousadas, hotéis e albergues, em todas as plataformas que o consumidor acesse posteriormente.

Todos estes exemplos remetem para o tema em questão, que é o Big Data. Atualmente, o *Big Data* tornou possível para empresas de diversos fins obterem informações e dados dos usuários que era impossível no passado, que hoje são utilizados para diversas finalidades. Desta forma, os usuários utilizam redes sociais e outras plataformas por hobby ou casualmente, e muitas vezes não sabem que seus dados estão sendo coletados. O problema é a falta de regulamentação sobre o tema, onde a lei permite que a empresa utilize os dados do titular sem informá-lo de tais utilizações.

Se sucede tal afirmação pelo previsto no § 4º, do Art. 7º, da Lei Geral de Proteção de Dados Pessoais¹³:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
[...] § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

E apesar de existir a previsão para dados tornados manifestamente públicos, uma outra problemática surge pelos atos dos próprios consumidores, uma certa insistência por parte da sociedade em geral em basicamente não se importar em ler

¹² BRASIL. Constituição. Constituição da República Federativa do Brasil - 1988.

¹³ Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais

os termos de utilização de aplicativos e muito menos de como os seus dados podem estar sendo compartilhados. Um exemplo claro e recente disto é o aplicativo *FaceApp*.

Feito provavelmente com o objetivo indireto de colher dados, se tem o *FaceApp*¹⁴, um aplicativo que surgiu no ano de 2019 e fora descoberto tempos depois que tinha como utilidade a coleta das fotos retiradas no mesmo. O aplicativo tinha a utilidade de editar a foto que o usuário tirava e transformar o usuário da foto como uma pessoa envelhecida. Neste caso específico do *FaceApp*, o próprio aplicativo demonstrava nos seus termos de utilização que tal situação poderia ocorrer.

A questão do *FaceApp* é importante para demonstrar o fato de que em inúmeros momentos, o usuário de aplicativos, redes sociais e outras plataformas, não tem a característica de procurar ler quais são os termos de comprometimento que aceita para usar um aplicativo ou plataforma.

O resumo é que com isso, sem muita regulamentação e também por falta de demonstração da importância do próprio usuário entender certos detalhes digitais, os usuários acabam por serem indiretamente totalmente vigiados pelo que tem interesse ou se deixa de ter, pelo que este usuário procura na internet.

Supostamente alguns benefícios desta coleta de dados pode ser caracterizada por uma vantagem para o usuário, mas ao menos tempo se viola a privacidade de cada um. É uma vantagem, pelo fato de "facilitar" o consumo de produtos e a busca de cada utilizador, mas ao mesmo tempo, se restringe em algumas plataformas como o *YouTube* e *Spotify*, sobre os vídeos e músicas que são recomendadas, o que dificulta muito a descoberta de novo conteúdo, pois não se sabe o motivo de tais recomendações surgirem para o usuário.

Desta forma, acaba por ser algo de certa forma perigoso e assustador para os usuários, se soubessem que podem há a possibilidade de se ter tanto acesso à vida do mesmo, muito menos quando não se sabe a finalidade, como foi o caso do *FaceApp*. Sendo assim, a regulamentação deveria ser mais rigorosa. A não utilização para discriminação deve ser evitada a todo custo e o consentimento deve

¹⁴ TechTudo - FaceApp rouba dados de usuários? Entenda termos de privacidade do app. Disponível em: <www.techtudo.com.br/noticias/2019/07/faceapp-rouba-dados-de-usuarios-entenda-termos-de-privacidade-do-app.ghhtml>.

ser essencial, além da transparência acerca da utilização do Big Data carecer de um grande aumento.

Seguindo nesta linha, com a transformação digital existente de forma mundial, atualmente no Brasil temos o Marco Civil da Internet¹⁵ e a Lei Geral de Proteção de Dados Pessoais¹⁶ para tentar auxiliar a área do Direito para a proteção dos dados. Outras legislações também podem ser mencionadas como a Lei "Carolina Dieckmann"¹⁷ que no caso, se tratava para crimes cibernéticos. Obviamente, mesmo tendo alguma legislação, ela não é nem perto de ser suficiente para a complexidade atual da situação.

Novamente, a maioria das pessoas não é atenta para os termos de utilização dos aplicativos e plataformas, mas mesmo que isso não seja uma desculpa para o tema, o correto seria a possibilidade na qual os utilizadores que não tem interesse em compartilhar os próprios dados, detivessem essa liberdade, mas muitas vezes para utilizar uma plataforma, o usuário automaticamente tem que compartilhar estes dados.

5 CONSIDERAÇÕES FINAIS

Para se evitar os perigos provenientes do *Big Data* essencialmente para a privacidade dos usuários, é fundamental primeiramente que estes dados sejam sempre coletados observando os princípios previstos na própria Lei Geral de Proteção de Dados, da finalidade, adequação, necessidade livre acesso qualidade dos dados, responsabilização e prestação de contas, transparência, segurança e prevenção.

Obviamente que a utilização da plataforma, para meios que não digam respeito ao compartilhamento de dados pessoais dos usuários, não diz respeito para necessárias mudanças ou criações de legislações sobre o tema, afinal a ferramenta do *Big Data* é de grande uso presente e futuro.

Para o que diz respeito ao compartilhamento de dados dos usuários e dos consumidores, observando os princípios, é possível que toda a mineração de dados

¹⁵ Lei n.º 12.965, de 23 de abril de 2014. Marco Civil da Internet.

¹⁶ Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais

¹⁷ Lei Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos.

seja com uma finalidade clara, específica e adequada, permitindo que aquele que é o titular dos dados tenha a capacidade de decidir se estes dados serão utilizados e demonstração das empresas que coletam estes dados para o usuário de todas essas situações.

Além disso, se torna necessária uma maior transparência no geral e uma ênfase para o utilizador quanto ao consentimento do mesmo para liberação destas informações, pois é notório que a maioria da população sequer entende ou sabe que suas informações estão sendo compartilhadas.

Também é importante destacar, a questão de uma possível "bolha" nas indicações que recebemos a partir da análise de nossos dados.

Esta "bolha", literalmente prende todos os usuários e consumidores no mesmo conteúdo, seja ele multimídia ou não e no mesmo tipo de produto, seja um que ele tenha adquirido anteriormente, ou não. Deveria haver opções em todas as plataformas para tais sugestões, para não ocorrer no caso do indivíduo estar sendo controlado indiretamente pela plataforma e sequer estar percebendo.

A ferramenta da internet e as tecnologias devem ser usadas para os seus benefícios de velocidade, extrema capacidade de informação e ampliação dos horizontes para os usuários. O uso da internet e seus domínios, amparado com uma política de monopolização do próprio pensamento dos seus usuários, apenas tende a eliminar toda opção de cada um e tornar cada vez mais, um indivíduo como uma cópia de outro, tirando da sua própria personalidade interesses, escolhas e preferências.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federal do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 jan. 2020.

_____. Lei n.º10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 20 janeiro. 2020.

_____. Lei n.º12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de**

dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 jan. 2020.

_____. Lei n.º12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jan. 2020.

_____. Lei n.º13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 jan. 2020.

_____. Lei n.º13.853, de 8 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.** Disponível em: www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 20 jan. 2020.

GÜNTHER, Wendy Arianne et al. **Debating big data: A literature review on realizing value from big data.** The Journal of Strategic Information Systems, v. 26, n. 3, p. 191–209, 2017.

PINHEIRO, Patrícia Peck. **Direito Digital**, 5 ed. rev. atual. e ampl. de acordo com as Leis n.º 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

TechTudo - **FaceApp rouba dados de usuários? Entenda termos de privacidade do app.** Disponível em: www.techtudo.com.br/noticias/2019/07/faceapp-rouba-dados-de-usuarios-entenda-termos-de-privacidade-do-app.ghtml. Acesso em 20 jan. 2020.