Utilização de dados pessoais pelas empresas: LGPD e o comportamento do consumidor com o macro modelo APCO

Use of personal data by companies: LGPD and consumer behavior with the macro model APCO

DOI:10.34117/bjdv7n6-641

Recebimento dos originais: 07/05/2021
Aceitação para publicação: 28/06/2021

Caroline Lujan de Oliveira
Mestranda em Administração
Universidade Federal de Rondônia – UNIR
Campus - BR 364, Km 9,5
CEP: 76801-059 - Porto Velho - RO
E-mail: carol-lujan@hotmail.com

Antonieta Ferreira Machado de Oliveira
Mestranda em Administração
Universidade Federal de Rondônia – UNIR
Campus - BR 364, Km 9,5
CEP: 76801-059 - Porto Velho - RO
E-mail: antonietamachado@hotmail.com

Carolina Yukari Veludo Watanabe
Doutora em Ciências de Computação e Matemática Computacional
Universidade Federal de Rondônia – UNIR
Campus - BR 364, Km 9,5
CEP: 76801-059 - Porto Velho - RO
E-mail: carolina@unir.br

RESUMO

Com este ensaio teórico, busca-se propor uma reflexão a respeito da privacidade de dados pessoais, destacando suas dimensões, bem como explanar algumas consequências do uso da internet, até mesmo inconsequentemente. As empresas utilizam informações sobre os clientes para ofertar serviços personalizados, no entanto, os consumidores que mais valorizam a transparência da informação, são os que menos possuem perfis *on-line* traçados para êxito das empresas na captação de clientes através desta singularidade. Conforme se destaca na literatura, ao estudar privacidade deve-se abordar o macro modelo denominado APCO (Antecedentes, preocupações com a privacidade e Resultados), o qual retrata que o contexto e a personalidade impactam na tomada de decisão de privacidade. Esboçamos ainda, alguns elementos sobre a proteção de dados pessoais, destacando que a emergência do fenômeno é resultado de uma série de fatores pressionados por lei para que as empresas adequem suas práticas a padrões internacionalmente rígidos. Concluímos com destaque às implicações de compreender práticas do uso da Internet, e consequências incalculáveis da circulação instantânea de dados que ela propicia, desdobrando possibilidades de estudos futuros.

Palavras-chave: Proteção de dados pessoais, LGPD, Direito à privacidade. Modelo macro abrangente.

ABSTRACT
With this theoretical essay, we seek to propose a reflection on the privacy of personal data, highlighting its dimensions, as well as explaining some consequences of internet use, even inconsequentially. Companies use information about customers to offer personalized services, however, consumers who most value the transparency of information are those who least have online profiles designed for the success of companies in attracting customers through this uniqueness. As highlighted in the literature, when studying privacy, the macro model called APCO (Background, Concerns with Privacy and Results) should be addressed, which portrays that the context and personality impact on privacy decision-making. We also outline some elements about the protection of personal data, highlighting that the emergence of the phenomenon is the result of a series of factors pressured by law for companies to adapt their practices to internationally strict standards. We conclude with emphasis on the implications of understanding practices in the use of the Internet, and the incalculable consequences of the instantaneous circulation of data it provides, unfolding possibilities for future studies.

Keywords: Personal data protection. LGPD. Right to privacy. Comprehensive macro template.

1 INTRODUÇÃO

Este artigo discorre sobre o prisma do direito à privacidade de dados pessoais de todo cidadão, e paralelamente, realçamos o grau de exposição que somos suscetíveis em decorrência do cotidiano informatizado que vivemos, tornando difícil efetivar o controle de dados.

O presente estudo consiste em um ensaio teórico caracterizado pela sua natureza reflexiva e interpretativa, utilizado como opção consciente e intencional, ou seja, como a forma mais adequada no entendimento de algo. Pesquisadores optam pelo ensaio, porque neste parece caber tudo, todo conhecimento é possível, a falta de rigor nas argumentações são mascaradas com a ideologia da liberdade total (MENEGHETTI, 2011).

Com o objetivo de facilitar os negócios, as empresas captam informações que suportem um fornecimento de serviço personalizado, a fim de captar a lealdade do consumidor, permitindo a redução da interação pessoal entre empresa e clientes, ou seja, realizam uma transparência da informação e personalização da privacidade. No entanto, a coleta de informações do consumidor pode levar a uma preocupação com sua privacidade, em como seus dados são armazenados e utilizados (AWAD; KRISHNAN, 2006).

A maioria dos sites usam informações pessoais para personalização de publicidade e um grande número de empresas conceituadas como *Google*, *Yahoo*, *Microsoft* e *Facebook* compartilham seus dados coletados de clientes com centenas de empresas afiliadas. Juntamente a esse uso e compartilhamento de dados, há uma associação de risco: na pesquisa de 2007 do Instituto Ponemon com uma amostra de 786 consumidores americanos, verificou-se que 62% dos os entrevistados foram notificados de que seus dados confidenciais estavam perdidos ou roubados e que 84% desses consumidores expressou maior preocupação ou ansiedade devido à perda de dados (SMITH; DINEV; XU, 2011).

Um exemplo recente é o caso do professor universitário David Carroll, um americano que utilizou as leis britânicas para processar a empresa de assessoria política Cambridge Analytica, que utilizou informações de usuários do *Facebook* para a criação de campanhas políticas. Em janeiro de 2019, a empresa foi considerada culpada pelo uso indevido de mais de 50 milhões de usuários do *Facebook*, no ano anterior. Utilizaram a Inteligência Artificial para formar perfis de eleitores e mostrarem o mundo como queriam e assim, mudar comportamentos e bombardeá-los com anúncios em uma plataforma onde as próprias pessoas cedem suas informações pelas redes sociais, fato que repercutiu no filme Privacidade Hackeada (*The great hack*), autores Karim Amer, Jehane Noujaim, lançado em julho de 2019. Fato este que demonstra grave ameaça à democracia (ARAÚJO; COUTO, 2021).

Com base na percepção de Smith *et al.* (2011), ao se tratar de privacidade, recomenda-se que os pesquisadores estejam atentos a um modelo macro abrangente que denominado APCO (Antecedentes → Preocupações com a privacidade → Resultados), o qual focaliza que antecedentes (geralmente, traços individuais ou fatores contextuais) levam indivíduos a formar preocupações com privacidade, e resultados comportamentais no processamento de informações do indivíduo. Dinev *et al.* (2015) propõe um modelo aprimorado de APCO e um conjunto de proposições relacionadas que consideram respostas cognitivas deliberadas, de alto esforço, e respostas cognitivas de baixo esforço inspiradas em estruturas e teorias em economia comportamental e psicologia.

Ressalta-se que este trabalho se destina a contemplar uma reflexão referente à privacidade de dados. Percebemos que existem pessoas preocupadas com a invasão de informações que ocorre através de publicidades personalizadas, como exemplo as plataformas de sites em que surgem aleatoriamente anúncios de produtos ou serviços de

interesse recente do consumidor na tela de seus aparelhos tecnológicos. Da mesma forma que empresas têm acesso para fornecer uma propaganda, o que garante que não possuam acesso e coletem dados arquivados nas máquinas utilizadas por estas pessoas, incluindo arquivos confidenciais?

2 PRIVACIDADE DE DADOS E SEUS REFLEXOS NA SOCIEDADE

Smith *et al.* (2011) observaram que quando o conceito de privacidade geral foi aplicado ao comportamento do consumidor, obtém-se um paradoxo de privacidade: apesar das preocupações com a privacidade relatadas, os consumidores ainda prontamente enviam suas informações pessoais em várias circunstâncias, e cooperam na coleta *on-line* de dados sobre si mesmos como assuntos econômicos.

Recursos de transparência de informações promovem um efeito sob a vontade do consumidor para obter ofertas personalizadas. Este efeito da transparência da informação sobre a disposição do usuário ocorre diante de perfis *on-line* e se difere entre serviço personalizado (que oferece uma arte personalizada ao cliente que tem interesse naquele objeto) e serviço de publicidade personalizado (que oferece uma arte sem interesse direto do cliente, porém tem possibilidade de captá-lo através de uma personalização conforme seus moldes de consumo).

Awad e Krishnan (2006) abordaram em seu trabalho as evidências empíricas de um paradoxo central para empresas que investem em personalização, utilizando a metodologia baseada na análise de 400 consumidores, três medidas para demonstrar a validade dos itens operacionais: unidimensionalidade, confiabilidade e validade discriminante e descreveram a preocupação com a privacidade do consumidor e a importância da política de privacidade, associado à importância da transparência da informação, sendo todos estes, itens necessários para o êxito de uma empresa.

O modelo original de APCO se baseia no processamento cognitivo de alto esforço, e pressupõe que comportamentos relacionados à privacidade são promulgados por meio de processos deliberados e de alto esforço, de maneira que o pesquisador encontra dificuldades em explicar conduta. Um modelo aprimorado APCO incorpora processamento de baixo esforço que envolve relativamente pouco esforço cognitivo, fornecendo um relato mais completo das atitudes, expõe que é inegável que os sentimentos distorcem o julgamento (DINEV *et al*. 2015). O comportamento é

caracterizado por uma racionalidade limitada (o que se reflete em termos coloquiais, como julgamentos “nublado” ou “apressado” na análise de custo-benefício).

Outro costume do indivíduo frequente pode ser explicado pelo viés do “sim” que é a prontidão com que as pessoas forneçam o número de telefone ou e-mail aos caixas em lojas sem sequer receber cartões de desconto ou cupons. As influências dos vieses otimistas e “sim” serão provavelmente observados diretamente em reações comportamentais. (DINEV *et al.*, 2015).

A teoria da maximização da utilidade, também conhecida como teoria da escolha racional, é um modelo de escolha do consumidor que não se expõe a riscos ou incertezas, levando a condições que ajudam a pessoa a prever o resultado de suas ações. Consumidores que tendem a não fazer um levantamento de custo-benefício financeiro, realizam contratos sociais com resultados imprevisíveis. Esta crítica remonta a década de 1960, onde era exposta uma dificuldade nas trocas sociais por não existir um valor preciso para as trocas e não existiam distinções claras entre o valor de uma troca social para outra (AWAD; KRISHNAN, 2006).

Dinev *et al*. (2015) constataram que pessoas estão esgotadas cognitivamente são mais propensas a usar atalhos cognitivos em vez de estudar, examinar e avaliar informações relacionadas à privacidade de informação. Na medida em que "ações fáceis" envolvem maior risco à privacidade, o esgotamento cognitivo pode colocar a privacidade das pessoas em risco. Por exemplo, após um dia longo e cansativo, uma pessoa pode postar uma mensagem ou imagem controversa no *Facebook* ou *Twitter* que leva a arrependimentos posteriores por esse post. A utilização dessas informações visualizadas por usuários em geral, pode tomar grandes proporções e gerar consequências desconhecidas.

A falta de leis regulamentares compromete a privacidade digital, e diante de tantos casos dessas violações divulgadas na mídia, foi proposta a Lei de Proteção de Dados com a finalidade de redução desta invasão de privacidade que permeia em todos os lugares e acessos conectados, desde aquisições on-line ao uso de redes sociais, de serviços hospitalares aos bancários, de escolas a teatros, de hotéis a órgãos públicos, da publicidade à tecnologia: é notório e global o entendimento de que a Lei Geral de Proteção de Dados Pessoais (LGPD) impactará diferentes setores e serviços, e a todos os brasileiros, seja no papel de indivíduo, empresa ou governo.

O advogado Alexandre Pacheco, em um bate papo com a FGV, menciona que atualmente, dados pessoais fazem parte de estratégias empresariais, de pesquisas acadêmicas, de iniciativas de transparências. E tendo em vista todo esse contexto, a lei cria formas de garantir controle de parte do titular, por exemplo, direito para o titular e deveres para agentes de tratamento de dados pessoais. A Lei de Proteção de Dados, no Brasil, apesar de ter sido aprovada em agosto de 2018, estava prevista para entrar em vigor a partir de agosto de 2020, entretanto dia 29 de abril de 2020, o presidente Jair Bolsonaro editou a Medida Provisória (MP) nº 959/2020 que trata da operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda que também prevê o adiamento da Lei nº 13.709 que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD), passando a valer apenas em maio de 2021. Onde será necessária mudança formal, documental, de postura e procedimentos internos das empresas e entes públicos, e essa flexibilização na legislação servirá para a manutenção de empregos, pois decorre da pandemia do Covid-19 que o mundo está enfrentando, anunciada em 11 de março de 2020 por Tedros Adhanom Ghebreyesus, diretor-geral da Organização Mundial da Saúde (OMS) (TAHO, 2020).

Diante esse contexto, entende-se a singularidade e seriedade desta Lei, porém proporcionará maior segurança jurídica em decorrência deste intuito em padronizar normas e práticas e promover proteção de dados, de forma unificada nacional e internacionalmente, de todo cidadão que esteja no Brasil. E, para maior esclarecimento, obtém-se inicialmente na LGPD a conceituação de dados pessoais, deliberando que dentre os dados há aqueles que são submetidos a cuidados ainda mais específicos, chamados de dados sensíveis, juntamente aos dados sobre crianças e adolescentes, e que são expostos à tratamento tanto nos meios físicos como nos digitais e ainda sujeitos à regulação.

Acrescenta-se ainda que a base da LGPD consiste no consentimento, ou seja, será necessário o cidadão consentir que seus dados pessoais sejam tratados, exceto se for indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão (SERPRO, 2020).

Dessa forma, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) dará suporte ao Brasil no quesito fiscalização, ao observar se a LGPD está sendo cumprida, caso contrário, poderá atribuir penalizações. Além disso, à ANPD serão atribuídas as funções de: regular e de orientar, preventivamente, sobre como aplicar a lei, tendo em vista que a população no geral poderá colaborar com a autoridade.

Por fim, como protagonista na questão de auxiliar o país na adequação aos princípios da LGPD e fomentar a construção das alternativas que o novo ordenamento traz para o Brasil dar um salto digital citamos o Serviço Federal de Processamento de Dados (SERPRO) definido como a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil, criada pela Lei nº 4.516, de 1 de dezembro de 1964, com objetivo de modernizar e dar agilidade a setores estratégicos da administração pública, a qual se compromete com a segurança e garantia da revolução tecnológica brasileira. E no intuito da observância de "boa-fé" destas ações, no artigo 6º da LGPD são descritos os 10 princípios que devem ser respeitados, elucidados na figura 1.

Figura 1 - Princípios da LGPD.

Fonte: Guedes (2020).

A figura 1 pontua os 10 princípios da LGPD, e conforme explica Guedes (2020):

1. Finalidade: toda atividade de tratamento de dados pessoais deve ser realizada com propósitos legítimos, específicos e informados ao titular.

2. Adequação: uma vez que a finalidade para o tratamento é bem determinada, este tratamento deve se manter compatível com o que foi informado ao titular.

3. Necessidade: o tratamento deve se manter limitado ao mínimo necessário para a realização da finalidade informada.

4. Livre Acesso: é mandatório garantir ao titular a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como da integralidade (precisão e consistência) de seus dados pessoais.

5. Qualidade: também é necessário garantir a exatidão, clareza, relevância e atualização dos dados de acordo com a necessidade e para o cumprimento da finalidade do tratamento.

6. Transparência: é essencial fornecer ao titular informações claras, precisas e facilmente acessíveis sobre a atividade de tratamento de seus dados e os agentes envolvidos.

7. Segurança: a empresa precisa demonstrar que é capaz de utilizar medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

8. Prevenção: a empresa precisa adotar medidas para prevenir eventuais danos decorrentes do tratamento de dados pessoais.

9. Não discriminação: o tratamento de dados não deve ser utilizado para fins discriminatórios ilícitos ou abusivos.

10. Responsabilização e prestação de contas: a empresa precisa saber demonstrar a eficácia das medidas adotadas e a adequação às normas.

Com isto, torna possível observar quão desafiador será adequar empresas que fornecem, por exemplo, serviços digitais e só conseguem melhorar seu lucro financeiro através do acesso aos dados dos consumidores. Entretanto, para gigantes do ramo da tecnologia se adequarão de maneira muito mais fácil por possuírem recursos e seus centros de negócios e atividades já estão focados em dados. E aproveitam dessa apropriação para melhorar o serviço prestado, modelando conforme a satisfação do cliente consegue fidelizar este consumidor, gerando um ciclo de oportunidades (KARWATZKI *et al.*, 2017).

Diante do elencado, complementamos que controlar a exposição de dados é praticamente impossível diante do mundo conectado, transformado após a revolução da tecnologia da informação. Vivemos numa realidade onde a conexão com o mundo digital

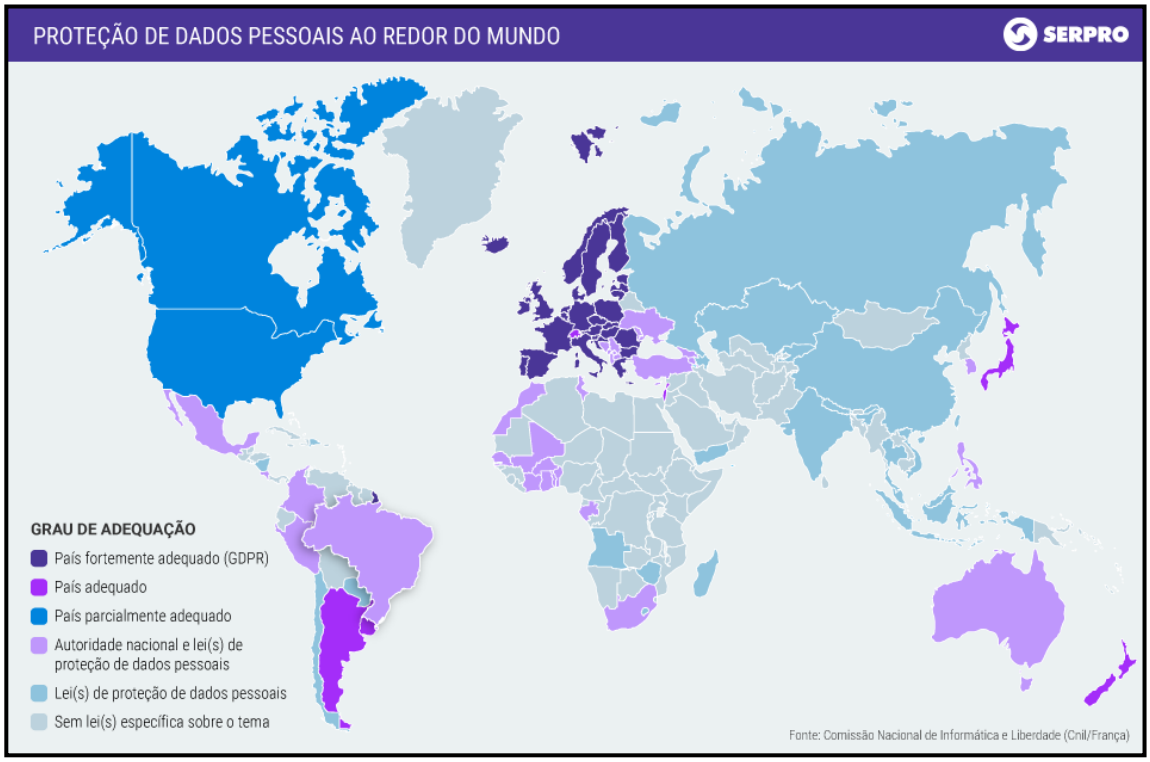
traz conforto e qualidade, de tal maneira que fazemos questão de usufruir desta comodidade.

A ausência de segurança de dados proporciona uma exposição incontrolável, levando a proporções imensuráveis, não existindo atualmente formas de controle do que pode ser divulgado, uma vez que a arquitetura da internet, apesar de demonstrar dados de segurança em várias transações, não é capaz de frear acessos de terceiros.

A invasão da privacidade de certas empresas chega a ser grande ao ponto de exigir do cliente informações como seu cadastro de pessoa física (CPF) e telefone para concluir a compra de um produto, pairando claramente um sentimento de impotência diante dessa coação ou limitação que estamos expostos corriqueiramente.

A seguir, na figura 2 é exposto o grau de adequação à LGPD no mundo no ano de 2020.

Figura 2 - Mapa de Proteção de Dados no Mundo.



Fonte: SERPRO (2020).

Com a figura 2 é possível observar, primeiramente, o destaque do continente europeu considerado fortemente adequado à LGPD em contrapartida, o continente africano definido em quase sua totalidade como “sem lei específica sobre o tema”. O Brasil encontra-se inserido em “autoridade nacional e lei(s) de proteção de dados

pessoais", significando que está passando por ajustes internos para a Lei entrar em vigência.

3 CONSIDERAÇÕES FINAIS

Dinev *et al.* (2015) mencionaram que situações em domínio público muitas vezes deixam os observadores perplexos quanto à forma como os indivíduos poderiam ser tão imprudentes a ponto de comprometer imagens, enviar mensagens em suas contas de redes sociais ou usar seus telefones celulares ou contas *on-line* para atividades ilegais. Nesses casos, esses indivíduos subestimaram o risco de seu comportamento, e é claro que esses indivíduos certamente estavam envolvidos no processamento de informações de baixo esforço, por exemplo, em intensos estados emocionais.

Neste contexto, também observamos que muitos usuários de contas *on-line* desconhecem os riscos aos quais se submetem, ou, a fim de se manterem conectadas, deduzem que estas privacidades de dados não podem ser captadas por fontes externas. As entrelinhas de termos e condições de aplicativos, programas, plataformas e outros podem conter solicitações que dão direitos aos programadores e empresas ao acesso dos dispositivos pessoais de cada cliente, como fotos, senhas e dados privados. Por exemplo, Smith *et al.* (2011) observaram uma conclusão normativa como "as sociedades devem reconhecer o direito à privacidade nas transações de compra" sem qualquer ligação clara aos resultados que seguiriam ou não desse direito.

Nós como usuários, adquirimos serviços de empresas que utilizam nossos dados para personalizar informações e gerar receitas e verificamos também que a conduta imprudente do uso da internet pode levar a consequências incalculáveis devido aos rastros digitais minados por indústrias e a quase impossibilidade de medir a própria privacidade, a ponto de não entendermos como nossos dados estão sendo usados, muitas vezes contra nós mesmos.

Acende-se um alerta para os dados tecnológicos expostos e crimes cibernéticos, onde os usuários estão reconhecendo os riscos do mundo virtual, preocupando-se em não arriscarem sua privacidade *on-line* através de comportamentos seguros. E cabe às empresas refazerem suas políticas e retomarem um conceito respeitável na tentativa de reconquistar a credibilidade de seus clientes.

REFERÊNCIAS

ARAÚJO, M.L.C; COUTO, W.H.O. New Technologies and Data Protection in Brazilian Democracy: between anarchy and normative control. **Brazilian Journal of Development**, v.7, n.6, p.55444-55456, 2021.

AWAD, N.F.; KRISHNAN, M.S. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization, **MIS Quarterly**. 2006.

BRASIL. Economia lança consulta pública para formulação da Estratégia de Governo Digital. **Ministério da Economia**, Publicado dia 08 de novembro de 2019. Disponível em: <http://www.economia.gov.br/noticias/2019/11/economia-lanca-consulta-publica-para-formulacao-da-estrategia-de-governo-digital>. Acesso em: 12 de novembro de 2019.

BRASIL. Medida provisória nº 959, de 29 de abril de 2020. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 29 abril 2020; 199º da Independência e 132º da República.

DINEV, T.; MCCONNELL, A. R.; SMITH, H. J. Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. **Information Systems Research**, 2015.

GUEDES, W. LGPD e marketing: guia prático para o profissional de marketing digital. DIGITALKS, 24 de agosto de 2020. Disponível em: < https://digitalks.com.br/artigos/lgpd-e-marketing-guia-pratico-para-o-profissional-de-marketing-digital/>. Acesso em 19 de abril de 20201.

MENEGHETTI, F.K. O que é um ensaio-teórico? Revista de Administração Contemporânea. Vol.15 no. 2, Curitiba Mar./Abr. 2011.

PAHO, OMS afirma que COVID-19 é agora caracterizada como pandemia. Organização Pan-Americana da Saúde (OPAS) – Brasil, 11 de março de 2020. Disponível em: <https://www.paho.org/bra/index.php?option=com_content&view=article&id=6120:oms-afirma-que-covid-19-e-agora-caracterizada-como-pandemia&Itemid=812>. Acesso em 06 de agosto de 2020.

KARWATZKI, S.; DYTYNKO, O.; TRENZ, M.; VEIT, D. Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization, **Journal of Management Information Systems**, 2017.

PACHECO, A. A Nova Lei de Proteção de Dados e o resguardo da privacidade. **https://www.youtube.com/watch?v=ldcR-XpYE8k&feature=youtu.be**

SERPRO. Em que "estágio" estamos? Confira o mapa da proteção de dados pessoais no mundo. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais>. Acesso em 15 de abril de 2021.

SERPRO. O que é a Lei Geral de Proteção de Dados Pessoais? Dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em 15 de abril de 2021.

SMITH, H. J.; DINEV, T.; XU, H. Information Privacy Research: An Interdisciplinary Review. **MIS Quarterly**. Vol. 35 No. 4/December 2011.

THE Great Hack. Direção de Karim Amer e Jehane Noujaim. Estados Unidos: Netflix, 2019. 133 minutos.