RECH- Revista Ensino de Ciências e Humanidades – Cidadania, Diversidade e Bem Estar. **ISSN 2594-8806**

Vol VII, núm. 2, jul-dez, 2023, pág. 463-483

A SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES: UM ESTUDO SOBRE O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA GESTÃO

SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES: UN ESTUDIO SOBRE EL IMPACTO DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN LA GESTIÓN

Roger Luz da Rocha[1]
Selma Velozo Fontes[2]
Thiago Fontes Machado[3]

RESUMO

Estudo bibliográfico que apresenta as implicações exercidas pela promulgação da lei que aborda o tratamento de dados pessoais nas organizações, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD). A lei específica passou a entrar em vigor em todo território nacional no ano de 2020. Diante deste cenário, o presente artigo aborda os objetivos e impactos da referida lei sobre as organizações. Para tanto, foram analisados estudos destacando-se os seguintes temas: segurança da informação, privacidade, vigilância, dados pessoais e gestão. O percurso metodológico baseou-se na revisão de literatura tendo como apoio a base de dados *web of science*, além disso o estudo tomou fontes secundárias como livros, *sites* eletrônicos e pesquisas de consultorias. Como resultado, constatou-se ao final do estudo que as empresas brasileiras não estão preparadas para adequação à nova lei, uma vez que há escassez de mão-de-obra qualificada, bem como diretrizes e políticas que integrem aspectos físicos, tecnológicos e organizacionais em suas práticas. Contudo, apesar dos impasses, a LGPD traz consigo benefícios em matéria de competitividade e seguridade jurídica internacional, sendo ela uma lei altamente aderente a realidade vigente.

Palavras-chave: Segurança da Informação; Privacidade; Vigilância; Lei Geral de Proteção de Dados Pessoais. Gestão.

RESUMEN

Estudio bibliográfico que presenta las implicaciones que ejerció la sanción de la ley que trata sobre el tratamiento de datos personales en las organizaciones, la denominada Ley General de Protección de Datos Personales (LGPD).

[1] Mestre em Administração pela Fundação Getúlio Vargas (FVG-EBAPE/RJ). Doutorando em Administração pelo Instituto de Pós-Graduação e Pesquisa em Administração da Universidade Federal do Rio de Janeiro (COPPEAD/UFRJ). E-mail: roger.ldr@gmail.com. Brasil. Lattes: http://lattes.cnpq.br/6773065088243542. ORCID iD: https://orcid.org/0000-0001-7261-101X.

[2] Mestre em Gestão e Estratégia de Negócios pela Universidade Federal Rural do Rio de Janeiro (UFRRJ). Docente (UFRRJ). E-mail: svfontes@ufrrj.br. Brasil. Lattes: http://lattes.cnpq.br/5006471121311105. ORCID iD: https://orcid.org/0000-0001-8195-4823.

[3] Graduando em Direito pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO). E-mail: thiago.machado@edu.unirio.br. Brasil. Lattes: http://lattes.cnpq.br/2688050568701891. ORCID iD: https://orcid.org/0009-0005-1421-4936.

La ley específica entró en vigencia en todo el territorio nacional en el año 2020. Ante este escenario, el presente artículo aborda los objetivos e impactos de la referida ley en las organizaciones. Para ello, se analizaron estudios, destacando los siguientes temas: seguridad de la información, privacidad, vigilancia, datos personales y gestión. El camino metodológico se basó en una revisión bibliográfica, apoyada en la base de datos web of science, además de esto, el estudio tomó fuentes secundarias como libros, sitios electrónicos y encuestas de consultoría. Como resultado, se encontró al final del estudio que las empresas brasileñas no están preparadas para adaptarse a la nueva ley, ya que hay escasez de mano de obra calificada, así como directrices y políticas que integren aspectos físicos, tecnológicos y organizacionales en sus prácticas. Sin embargo, a pesar de los impasses, la LGPD trae consigo beneficios en términos de competitividad y seguridad jurídica internacional, por ser una ley muy adherente a la realidad actual.

Palabras clave: Seguridad de la Información; Privacidad; Vigilancia; Ley General de Protección de Datos Personales. Gestión.

1. INTRODUÇÃO

A vigilância é um tema frequentemente retratado nas notícias, assim como em produções culturais. Assumindo características mutáveis, é possível encontrá-la nos variados segmentos midiáticos (filmes, programas de TV, *reality shows*, séries, entre outros). Nos últimos anos, nota-se um crescente interesse por parte da sociedade sobre o fenômeno, justificado pelas inúmeras polêmicas e escândalos envolvendo crimes cibernéticos de invasão de privacidade, bem como de vazamentos de dados pessoais sensíveis.

Conforme Castells (2011), os indivíduos vivem em uma sociedade em rede altamente conectada ao universo digital no qual os dados são considerados fontes geradoras de riqueza e poder. Os dados tornaram-se bens econômicos valiosos. O 'Dataísmo', termo cunhado por Harari (2016), refere-se justamente ao protagonismo atribuído ao fluxo de informações extraídos do Big Data[4]. Além disso, o autor destaca o vasto campo de atuação de tais ferramentas de análise e monitoramento de dados perpassando os diferentes campos do tecido social (saúde, educação, segurança, universo empresarial, relações sociais etc.).

Empresas do setor de tecnologia, em especial, *Google*, *Facebook*, *Amazon*, *Tencent*, *Baidu*, *ByteDance* entre outras gigantes do segmento perceberam o valor da mineração de

[4] *Big Data* é um conceito que descreve o grande volume de dados estruturados e não estruturados que são gerados a cada segundo. Disponível em: <http://marketingpordados.com/analise-de-dados/o-que-e-big-data-%F0%9F%A4%96/>. Acessado em: 26 ago. 2020.

dados, e, com isto, inauguraram uma nova lógica de acumulação capitalista baseada na extração de dados pessoais por intermédio da vigilância (ZUBOFF, 2019).

Cada vez mais as empresas de tecnologia desenvolvem algoritmos, dispositivos tecno-inteligentes capazes de predizerem comportamentos, gostos, predileções, hábitos, e, até mesmo, delineiam o perfil psicossocial dos indivíduos. Em 2019, o aplicativo TikTok teve que pagar uma multa milionária por violação de privacidade envolvendo captação de dados pessoais de menores. Ademais, o aplicativo utiliza de algoritmos de *machine learning* para personalizar seu conteúdo com intuito de descobrir mais a respeito do comportamento, hábitos e gostos de seus usuários (EL PAÍS, 2020)[5].

O episódio mencionado acima, expressa a importância do estudo, pois evoca o dilema ético envolvendo a preservação da privacidade no mundo contemporâneo, impasse este, reforçado pelo poder de vigilância, de acordo com Foucault (2002), que as corporações impingem sobre os indivíduos ao compartilhar voluntariamente informações pessoais na *web*.

A dinâmica de vigilância sofisticou-se de tal maneira que o caso emblemático da *Cambridge Analytica/Facebook* é considerado obsoleto, segundo Harari (2020), face aos novos aparatos disponíveis no momento. Hoje, há um monitoramento constante, por meio da rastreabilidade de dados pessoais, no qual indivíduos passaram a ser vigiados a todo momento.

A democratização da vigilância liderada pela indústria ou economia da vigilância, esbarra em dilemas éticos, sobretudo, em termos de garantia de proteção à privacidade, sigilo e sobre o direito de esquecimento. Vale ressaltar que a 'anonimização' se tornou uma 'anomia social', no sentido apregoado pelo sociólogo francês Émile Durkheim, ou seja, um comportamento fora do padrão social, pois o discurso atual é de livre compartilhamento das informações segundo Han (2017), no entanto, tal atitude sem limites, viabiliza precedentes para o surgimento de transgressões à dignidade da pessoa humana.

[5] SANTIRSO, J. O lado obscuro do Tik Tok, a rede social chinesa dos vídeos curtos: Aplicativo tem 500 milhões de usuários, mas sua origem desperta dúvidas sobre a segurança dos dados e a liberdade de do conteúdo. Disponível em: <https://brasil.elpais.com/tecnologia/2020-01-19/o-lado-escuro-do-tiktok-a-rede-social-chinesa-dos-videos-curtos.html>. Acessado em: 27 ago. 2020.

Inseridos na dinâmica tanto econômica quanto cultural, o modelo pan-óptico idealizado por de Bentham[6] toma novas formas e passa agir sob novas teias, isto é, com atuações no universo digital. A hipervigilância ganha força pondo em xeque valores ocidentais fundamentais, bem como produz novas formas de interações sociais e subjetivação nos indivíduos (BAUMAN e DONKIS, 2014; HAN, 2017).

Outros eventos icônicos envolvendo abuso contra a privacidade foram denunciados pelo ex-agente da CIA, Snowden, 2013, revelou o programa de espionagem e vigilância global do governo norte-americano – Sistema ECHELON – rede de monitoramento que esbarra contra o sigilo empresarial e de pessoas. Por fim, e não menos importante, Assange, 2006, fundador do *WikiLeaks* expôs preocupações com a massificação da vigilância também desvelando transgressões a privacidade entre outras questões complexas.

Nesse sentido, a sociedade atual é marcada pela vulnerabilidade de mecanismos regulatórios mais robustos que resguardem a integridade da pessoa humana, e, ao mesmo tempo que evitem violações a vida privada dos indivíduos no mundo digital. Cada vez mais as pessoas estão mais suscetíveis às invasões cibernéticas ou deturpações dos Estados quando teoricamente seriam estas instituições, responsáveis por zelarem pelos seus concidadãos e pela coisa pública.

A inseparabilidade entre o público e o privado, o mundo virtual e o mundo real são marcas da sociedade contemporânea. Caracterizada pela confusão existente entre o mundo real com o mundo digital, na realidade ambos os espaços que antes eram bem demarcados, hoje se sobrepõem, isto é, estamos *online* e *offline* simultaneamente (LEE, 2018).

Embora a segurança da informação nas organizações não seja algo inovador, conforme apontam Vasarhely e Mock (1974) é ainda um campo subaproveitado, principalmente, pelo seu potencial de trazer à tona reflexões, além de ser um recurso estratégico valioso para qualquer empresa. Dessa forma, as empresas precisam adotar diretrizes e políticas de segurança, pois são vitais para garantir a continuidade do negócio assim como a sua confiabilidade junto aos demais *stakeholders* (GORDON e LOEB, 2002; SÊMOLA, 2014).

[6] O modelo carcerário idealizado originalmente por Bentham consistia em uma torre posicionada estrategicamente na região central do presídio, cuja função corresponderia a metáfora do "olho que tudo vê", ou seja, observação plena. Em virtude disto, o conceito "panóptico" foi amplamente utilizado por Foucault (2002) como forma de caracterização das dinâmicas de poder próprias à sociedade moderna.

Finalmente, o estudo pretende investigar os impactos da Lei Geral de Proteção de Dados Pessoais (LGPD) para as empresas, principalmente, aspectos relacionados aquelas empresas que lidam diretamente com a extração e o monitoramento de dados pessoais. Com uma abordagem sistêmica, o estudo visa discutir a temática da segurança da informação ao referido problema, provocando a seguinte reflexão: como as empresas estão lidando com a implementação da LGPD em seus negócios? Ou ainda: em que medida as empresas estão preparadas para o tratamento e gestão dos dados pessoais em suas corporações?

2. REFERÊNCIAL TEÓRICO

Esta seção tem como objetivo abordar os principais conceitos e aspectos relacionados às práticas de vigilância que por sua vez esbarram sobre a privacidade das informações e sobre os dados pessoais salvaguardados pela Lei Geral de Proteção de Dados Pessoais.

2.1. Vigilância, Privacidade e os Dados Pessoais: Conceitos e Características

O romancista inglês George Orwell jamais iria supor o quão profético sua obra, 1984 seria para a contemporaneidade. A trama do romance baseia-se em uma sociedade regida por um governo totalitário, no qual os indivíduos são vigiados constantemente pela figura do "*Big Brother is wathcing you*". Esse cenário distópico, digno de cinema ou das artes não está tão distante da atualidade, muito pelo contrário, eventos envolvendo vazamento e violações de privacidade são noticiadas com certa frequência.

De acordo com Bauman e Lyon (2013), a vigilância é uma dimensão-chave no mundo contemporâneo, presente em todos os países, há uma proliferação de aparelhos e dispositivos como câmeras, escâneres corporais, checagem biométricas, senhas eletrônicas entre outras tecnologias de vigilância empregadas corriqueiramente. Nesse sentido, o contexto atual é marcado pela intensificação da vigilância, portanto, estamos inseridos em uma cultura da vigilância, conforme explica Lyon:

> Por cultura da vigilância, refiro-me aos tipos de coisas que um antropólogo pode estudar - costumes, hábitos e maneiras de olhar e interpretar o mundo. O foco está na vigilância sobre a vida cotidiana, e não, principalmente, nos tentáculos de polvo da inteligência global e nas redes de policiamento ou nas sirenes sutis e sedutoras do marketing corporativo. Compreendido aqui, a cultura da vigilância é sobre como a

> vigilância é imaginada e experimentada, e sobre como as atividades mundanas de andar na rua, dirigir um carro, verificar se há mensagens, comprar em lojas ou ouvir música são afetadas e afetam a vigilância. E sobre como a vigilância também é iniciada e envolvida por aqueles que se familiarizaram e até mesmo se acostumaram com a vigilância (LYON, 2018, p.10, tradução nossa)[7].

Inseridos nessa conjuntura, segundo Lyon (2018), a vigilância tornou-se um 'estilo de vida' tão difundido na sociedade que os indivíduos são expostos, e, ao mesmo tempo utilizadores, isto é, são afetados e agentes de vigilância concomitantemente. Vale ressaltar que muitos o são conscientemente, entretanto, outros não o são, uma vez que não percebem seus efeitos nocivos. Tais disparidades emergem por conta da capacidade mutante, fluída, em constante mudança, a isto, Bauman e Lyon (2013) atribuíram o termo de 'vigilância líquida'.

A disseminação do monitoramento tomou proporções grandiosas após o atentado de 11 de setembro, durante o governo George W Bush acentuou-se suas práticas, justificada pelo combate ao terrorismo. Além disso, o então presidente assinou o Ato Patriota, 2001, e desenvolveu um programa de vigilância global chamado, *Total Information Awareness* (TIA) em 2003. Desde então, novos outros projetos foram sendo revelados após Assange,2006, e Snowden, 2013.

Mecanismos de vigilância social e coleta de dados emergem e se sofisticam. Novas tecnologias são empregadas e outras tantas desenvolvidas em parceria com a iniciativa de empresas privadas gerando uma série de distorções e violações de privacidade, bem como de direitos fundamentais. Vide exemplo do supermercado Lidl[8] , boneca Cayla[9] , *Google Nest* do *Google*[10] , Alexa da *Amazon*, *Facebook*, Pokémon *Go*, TikTok, entre outros.

---

[7] By the culture of surveillance, I refer to the sorts of things that an anthropologist might study – customs, habits and ways of looking at and interpreting the world. The focus is on surveillance in everyday life rather than, primarily, in the octopus tentacles of global intelligence and policing networks or the subtle and seductive sirens of corporate marketing. Understood here, the culture of surveillance is about how surveillance is imagined and experienced, and about how mundane activities of walking down a street, driving a car, checking for messages, buying in stores or listening to music are affected by and affect surveillance. And about how surveillance is also initiated and engaged by those who have become familiar with and even inured to surveillance (LYON, p.10, 2018).

[8] DW. Rede alemã de supermercados é acusada de espionar funcionários. Disponível em: <https://www.dw.com/pt-br/rede-alem%C3%A3-de-supermercados-%C3%A9-acusada-de-espionar-funcion%C3%A1rios/a-3218032>. Acessado em: 26 ago. 2020.

[9] BBCBrasil.com. *Autoridades alemãs fazem alerta contra boneca que pode ser hackeada para espionar crianças.* Disponível em: <https://www.bbc.com/portuguese/internacional-39007610>. Acessado em: 26 ago. 2020.

[10] SANTINO, R. Google inclui microfone "secreto" em produto doméstico e não avisou usuários. Olhar digital, 2019. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/google-incluiu-microfone-secreto-em-produto-domestico-e-nao-avisou-usuarios/83026>. Acessado em 26 ago. 2020.

Afinal, como definir a vigilância? A etimologia da palavra vigilância provém do francês *surveiller*, cujo significado consiste em "vigiar, assistir" (LYON, 2001, p.3). Nesse sentido, a vigilância consiste tanto em cuidado como controle. Dessa forma, "o termo implica uma relação assimétrica de poder, controle, hierarquia, violência e dominação" (FUCHS, 2011, p.133). Partindo da mesma premissa, Foucault (2002), compreende a vigilância como uma técnica de coerção, na qual se estabelece uma relação de poder exercida através da supervisão.

Vale frisar que nem toda vigilância é maléfica, detentora de duas facetas, ela é "desengajadora assim como facilitadora" (ZUREIK, 2003, p.42). De caráter universal, é um fenômeno identificado em todas sociedades, responsável pela sociabilização e formação cultural através da vigilância dos adultos (NORRIS e ARMSTRONG, 1999, p.5). Portanto, seu caráter facilitador aliado ao aspecto restritivo é explicitado:

> A vigilância pode servir para fins de proteção, administração, cumprimento de regras, documentação e de estratégias ao mesmo tempo em que para objetivos relacionados a manipulação inapropriada, a limitar oportunidades de vida, ao controle social e à espionagem. [...] Em graus variados, a vigilância é uma propriedade de qualquer sistema social – seja entre dois amigos, num local de trabalho ou num governo (MARX, 2007, p. 535).

Com o crescente avanço tecnológico, mecanismos, técnicas algorítmicas e dispositivos mais sofisticados emergiram agravando ainda mais o fenômeno de monitoramento. Graças a convergência digital, segundo Jenkins (2009), pelo qual tudo passa a estar conectado à internet (*Internet of Things*) conjugado à infinidade de dados coletados (*Big Data*) facilita o uso de técnicas sofisticadas envolvendo sistemas inteligentes (AI) direcionados para personalização de produtos e serviços em diferentes áreas.

Diante disto, todos os dados pessoais passam a ser coletados, de acordo com Wolf (2010), em sintonia com o modelo pan-óptico idealizado por Bentham (2008). O setor econômico percebeu os ganhos, principalmente, empresas ligadas ao ramo tecnológico (*Google, Amazon, Facebook, Tencent*, etc.) e desenvolveram modos de rastreabilidade de dados pessoais para benefício de seus negócios: "[...] a vigilância econômica sobre informações privadas e sobre o comportamento on-line exercido por empresas no ramo de internet como

Facebook, *Google*, etc. para acumular capital com publicidade direcionada" (FUCHS, 2011, p.126).

A indústria da vigilância atualmente conta com companhias especializadas na obtenção do histórico de informações dos indivíduos e desenvolvem desde algoritmos até tecnologias vigilantes. Essas companhias são responsáveis pela exposição, e, ou venda das informações dos indivíduos, estabelecendo uma relação de poder sobre eles, que pode configurar-se como uma perda degenerativa da sua própria condição humana: perda de autonomia e dignidade (KANT, 1974). O ser humano, nessa nova lógica capitalista, chamada de 'Capitalismo de Vigilância', segundo Zuboff (2019), passa a ser um produto comercializável (BAUMAN, 1999; MARX, 2004).

De acordo com Zuboff (2019), o Capitalismo de Vigilância surge nos anos 2000, mais precisamente no Vale do Silício com as experiências do *Google* envolvendo mineração e coleta de dados pessoais. Por meio de inúmeras tentativas e erros, a empresa descobriu formas de monetização desses dados pessoais através da vigilância.

Ao recolherem informações individuais, o *Google* pode estabelecer traços comportamentais, perfis psicossociais, gostos, hábitos, preferência, hobbies, mas, acima de tudo, fomentou o desenvolvimento de um mercado de padrão comportamental (modelo de negócios). Como consequência, inúmeras transgressões à privacidade, foram encetadas pondo em xeque a vida íntima e o próprio valor de dignidade humana das pessoas. Diante disto, em 2016, a União Europeia elaborou a *General Data Protection Regulation* (GDPR) com intuito de regulamentar e salvaguardar o valor da dignidade humana e a vida privada de seus cidadãos (ZUBOFF, 2019).

Por seu turno, em 2018, o Brasil também institui a Lei Geral de Proteção de Dados Pessoais (LGPD) que entrou em vigor no país em 2020. Tanto a iniciativa europeia quanto a brasileira sinalizam zelo com a intimidade dos cidadãos e vão de encontro com a Declaração Universal dos Direitos Humanos (DUDH), "ninguém será sujeito em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo

ser humano tem direito à proteção da lei contra tais interferências ou ataques" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948, artigo 12)[11] .

A fim de evitar potenciais distorções empresariais, por conseguinte, proteger a segurança da informação dos indivíduos, o artigo 5º da LGPD, considera dado pessoal como toda "informação relacionada a pessoa natural identificada ou identificável" (LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS, 2018, artigo 5º, inciso I)[12].

Com a nova lei (LGPD, 2018), é preciso que haja consentimento prévio por parte dos titulares dos dados, desse modo mitiga-se as potenciais violações ou práticas de vigilância "qualquer recuperação e processamento de dados pessoais, seja identificável ou não, para os propósitos de influenciar ou gerenciar aqueles cujos dados foram recuperados" (LYON, 2001, p.2).

O mesmo raciocínio de resguardo à privacidade é prescrito na Constituição Brasileira de 1988: "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" (CONSTITUIÇÃO FEDERAL BRASILEIRA, 1988, artigo 5º, inciso X).

O fato é que a informação se tornou um produto economicamente valioso, segundo Ramonet (2003), e, concomitantemente, objeto de poder e rastreabilidade para as organizações (TOFFLER, 2003). Atualmente, existem tecnologias aptas a revelar detalhes da vida alheia (obtenção de dados pessoais). Diante de tal fato, o presente estudo visa analisar os desdobramentos éticos e legais tratados pela LGPD no tocante ao manuseio e tratamento dos dados pessoais em seus processos.

Dessa forma, a seção procurou traçar um breve panorama sobre a massificação da vigilância. Abordou-se o conceito relacionado a cultura da vigilância, dados pessoais, privacidade e o surgimento da sociedade da vigilância, isto é, a emergência de uma nova lógica capitalista baseada na extração e monitoramento de dados comportamentais, o assim chamado

[11] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Paris: Artigo 12º, 1948. Disponível em: <https://nacoesunidas.org/artigo-12-direito-a-privacidade/>. Acessado em: 27 ago. 2020.

[12] BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709). Brasil: Artigo, 5º, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acessado em: 27 ago. 2020.

capitalismo de vigilância. Na próxima seção, será abordado o papel e os impactos relacionados a LGPD nas organizações.

2.2. A Lei de Proteção de Dados Pessoais

Esta seção tem como objetivo destacar o papel da LGPD e seus desdobramentos nas organizações, sobretudo, pela sua exigência legal de adequação a partir de agosto deste ano. Ademais, serão explicitados os benefícios e reveses advindos da sua implementação, assim como serão identificados os impasses relacionados a sua adesão nas empresas. Por fim, a presente seção tecerá a evolução cronológica da LGPD, isto é, a fonte de inspiração para o seu desenvolvimento.

2.2.1. O impacto da LGPD sobre as organizações

Dado o contexto de profusão tecnológica, novos desafios têm surgido, principalmente relacionados a privacidade dos indivíduos na rede que frequentemente têm sido alvos constantes de ataques e infrações por *hackers* entre outros cibercriminosos. Dessa forma, visando proteger as informações pessoais, o poder público brasileiro percebendo a ausência de uma regulamentação específica inspirou-se na lei europeia *General Data Protection Regulation* (GDPR, 2016).

Em 2018, o Brasil instituiu a regulamentação da matéria, por meio da elaboração da Lei Geral de Proteção de Dados Pessoais (LGPD, 2018), na qual abarca exclusivamente sobre a coleta, extração, armazenamento e tratamento de dados pessoais no meio físico quanto digital. Em vigor a partir deste ano, a lei trouxe consigo desafios para as organizações e muitas questões referentes a sua devida adequação, pois esta tornou-se compulsória recentemente após alterações e aprovação em 2019, entretanto, cabe analisar quais são os obstáculos e impactos oriundos em virtude de sua obrigatoriedade em todo território nacional.

Assim, a LGPD (2018), demarcou as fronteiras de coleta, extração, armazenamento, acesso e tratamento dos dados que ocorrerão somente mediante o consentimento integral dos indivíduos. Portanto, as organizações precisam ser transparentes e informar a finalidade da coleta de dados, por quanto tempo será armazenado no banco de dados e quem será o

responsável pelo acesso, tais precauções são para garantir a privacidade individual. Em resumo, toda e qualquer informação identificável é considerada dado pessoal, sendo assim encontra-se resguardada pela legislação específica (LGPD, 2018).

As empresas precisam se adequar à nova lei, do contrário, impactos, sanções e multas severas podem ser aplicadas aos negócios. Dessa forma, o modo como as organizações lidam com os dados pessoais precisam estar em conformidade com os dez princípios norteadores da LGPD. A seguir, tem-se o quadro 1 que salienta e correlaciona as atividades de tratamento de dados e seus potenciais impactos as empresas.

Quadro 1: Desafios e impactos da LGPD nas organizações

Princípios norteadores da LGPD	Descrição	Desafios e impactos nas organizações
Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	O setor de marketing, telemarketing, de um modo geral serão um dos setores mais afetados, pois os dados dos clientes não poderão ser alvo de ofertas e publicidade, se houver desacordo com sua finalidade inicial.
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Modelos de negócios distintos somente poderão realizar pedidos de dados que estejam compatíveis ao seu contexto de negócio. Uma empresa de comércio eletrônico não estará autorizada a solicitar dados de saúde aos clientes, por exemplo.
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;	Nesse caso, o grau de responsabilização perante a organização será diretamente proporcional a quantidade de dados tratados pela corporação. Sugere-se nesse sentido, parcimônia.
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	Criação de processos enxutos e alinhados com uma política de segurança da informação serão necessários. Além disso, investimentos em sistemas de informação, bem como na contratação e treinamento de profissionais especializados serão necessários.
Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a	Investimento em tabelas e processos de temporalidade, assim como em pessoal atualizado e comprometido com a melhoria contínua dos dados.

	necessidade e para o cumprimento da finalidade de seu tratamento	Instauração de uma cultura de sigilo e proteção à privacidade. Por fim, investimentos em softwares ágeis e mecanismos de verificação dos bancos de dados existentes.
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;	Incentivo a uma política de segurança da informação e diretrizes que impeçam o compartilhamento de dados de titulares a terceiros, inclusive, parceiros e operadores. Boa comunicação, novos processos administrativos e tecnológicos precisam estar alinhados.
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;	Compor uma boa equipe de segurança da informação e cibersegurança será crucial. Técnicas de criptografia, medidas de conscientização em segurança da informação e boas práticas relacionadas a ISO/IEC 27001-2 devem ser adotadas. Investimentos em *softwares*, equipamentos e medidas de proteção física, organizacional e tecnológica são necessários.
Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Planos e diretrizes relacionados à segurança da informação para que se evite uma perda de credibilidade, confidencialidade e disponibilidade da informação e sigilo de seus titulares. Danos devido a um incidente pode causar desde a perda de credibilidade até multas severas e sanções legais. Por conta disto, compra de *softwares* de proteção, backups constantes, uso de sistema de criptografia e pessoal treinado e qualificado são ativos a serem investidos.
Não discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos	Em especial o setor de Recurso Humanos será afetado, uma vez que o setor dispõe dos dados pessoais sensíveis de seus funcionários ou clientes. Dessa forma, é preciso que exista uma política de combate à discriminação de qualquer prática abusiva, discriminatória. Por exemplo, currículos durante o processo de recrutamento ou seleção não podem exigir CPF, RG, fotos, gênero, filiação partidária e

		religiosa, raça, orientação sexual, registros biométricos etc.
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.	Contratação de consultorias especializadas, adoção de protocolos de segurança, treinamentos para a conscientização de pessoal, obter ISO/IEC 27001-2 entre outras medidas de segurança que podem ser atestadas.

Fonte: Elaborado pelos autores

Sendo assim, o maior risco em relação ao descumprimento da nova lei de proteção de dados pessoais, concerne em uma multa de 2% do faturamento a R$ 50 milhões, ou ainda, a suspensão das atividades da empresa, conforme expresso na lei (LGPD, 2018).

Portanto, além dos desafios impostos pela compulsoriedade da LGPD nas empresas, outra dificuldade encontrada, consiste em sua implementação. De acordo com Half (2019), é possível adotar a seguinte estratégia de adequação nas organizações: conhecer e entender a LGPD; definir um profissional responsável pela proteção de dados pessoais; informar e treinar colaboradores; obter consentimento para tratamento dos dados; revisar políticas de segurança da informação, contratos e dados já coletados; desenvolver uma cultura de proteção de dados e relatório de impacto; criar processos tecnológicos e operacionais para zelar pelos dados; ter uma estratégia de resposta para atender aos titulares de dados e à fiscalização.

Dentre os obstáculos apresentados, de acordo com o Half (2019), o gargalo no quadro de pessoal é considerado um dos maiores impasses da atualidade, pois cerca de 53% das empresas não estão preparadas para adesão a nova lei. Segundo a pesquisa de Half (2019), cerca de 34% dos gestores declararam que suas companhias não estão preparadas para a LGPD, outros 19% afirmaram que desconhecem do que se trata a nova lei. Dessa forma, o principal gargalo ao entrave da nova lei reside justamente no quadro de pessoal qualificado a nova realidade.

Se por um lado a LGPD traz obstáculos e reveses, por outro lança mão de benefícios e vantagens significativos para as corporações, conforme aponta o quadro 2 contendo as vantagens e desvantagens para o meio corporativo.

Quadro 2: Vantagens e desvantagens da aplicação da LGPD no meio corporativo

Vantagens	Desvantagens
Segurança	Desinformação
Maior confiança do consumidor	Custo
Melhor alinhamento com a evolução tecnológica	Burocracia
Melhor tomada de decisão	Controle externo
Nova cultura empresarial	Multas e sanções

Fonte: Elaborado pelos autores baseado em Break (2020)

Finalmente, a seção procurou traçar os impactos e desafios relacionados com a aplicação obrigatória da LGPD no universo empresarial. Observou-se, além dos impasses, vantagens e estratégias de adequação à nova realidade para as empresas brasileiras. Por fim, na próxima seção, será abordada a metodologia empregada na pesquisa.

3. METODOLOGIA

O objetivo do artigo é analisar os impactos da LGPD sobre as empresas e seus respectivos desdobramentos englobando desde sua adequação às exigências legais até sua implementação nas organizações. Com base nas características do objeto de estudo, a pesquisa empregada é do tipo qualitativa, pois a investigação procurou examinar e compreender o fenômeno causado da nova lei sobre o modelo de negócios da empresa, para isto, o cruzamento de dado qualitativo se apresenta como opção estratégica a fim de compreender e examinar o panorama enfrentado pelas empresas com a obrigatoriedade legal em suas práticas diárias.

A fim de compreender os efeitos da LGPD no cenário organizacional contemporâneo, o estudo recorre a pesquisa bibliográfica, pois esta explicito os impasses e desafios trazidos pela nova lei para o interior das corporações.

Segundo Vergara (2009), o percurso metodológico deve abarcar uma lógica de pensamento a ser seguida. Sendo assim, o caminho metodológico empregado adota sua taxonomia fundamentada em dois aspectos: quanto aos fins e quanto aos meios. Quanto aos fins – trata-se de uma pesquisa exploratória e descritiva. Exploratória, pois com a adoção recente da nova lei (LGPD), há uma carência de estudos nacionais que abordem seus impactos sobre as empresas. Descritiva, pois visa descrever os efeitos, percepções, sugestões,

expectativas de profissionais ligados ou afetados por sua implementação corporativa. Quanto aos Meios – trata-se de uma pesquisa bibliográfica visto que foi explorado materiais de domínio público em geral que estão intimamente correlacionados a LGPD nas empresas, tais como: artigos, livros, periódicos, teses e dissertações, dados de pesquisas publicados por entidades e instituições.

Para atender e alcançar os objetivos da investigação, o presente estudo, realizou uma revisão sistemática de literatura sobre dados pessoais nas empresas, selecionando, identificando e examinando pesquisas de relevância, com intuito de assegurar aporte teórico-empírico para análise da pesquisa bibliográfica executada. A pesquisa bibliográfica, conforme Gerhardt e Silveira (2009), trata-se de um levantamento dos principais estudos elaborados e publicados a respeito de um determinado campo científico pelo qual são obtidos conteúdos acumulados sobre a temática de investigação específica.

Os critérios adotados que serviram de apoio para a pesquisa bibliográfica do presente estudo foram: I) anos da publicação (2014-2020); II) adequação do título e do resumo com os objetivos propostos pelo estudo aqui apresentado; III) idiomas (inglês e português); IV) relevância dos achados da pesquisa.

A base de dados utilizada se deu por intermédio da base de periódicos da Capes, mais especificamente, envolvendo a base internacional: *web of science*. A escolha deve-se pelo renome internacional, além de contar com um repositório vasto de artigos revisados por pares (*peer review*) garantindo-se credibilidade científica aos estudos.

Empregou-se os operadores lógicos associados com as palavras-chaves respectivamente "*personal data*" *AND "data protection" AND "privacy*", o que culminou com total de 50 artigos revisados por pares e que teve como filtro os parâmetros mencionados anteriormente, assim como o filtro por área específica de estudo: *Business, Management and Law*, conforme observado no quadro 3. Desse modo, do total de 50 artigos, somente 28 atenderam os critérios de análise integralmente. Por fim, somando-se a isto, foram consultados estudos e pesquisas realizados por empresas de consultoria, assim como outras fontes secundárias tais como: livros, sites eletrônicos relacionados ao tema, justamente para cobrir o déficit de produções nacionais que aprofundassem o estudo.

Quadro 3: Composição dos artigos nas Bases de dados empregadas

Base de Dados	Total de artigos	Artigos analisados
Web of Science	50	28
Total:	50	28

Fonte: Elaborado pelos autores com base na *Web of Science* (2020)

Portanto, a seção procurou definir e explicar o caminho metodológico a ser traçado com o propósito de responder o problema de pesquisa bem como adequá-lo ao objetivo da investigação.

4. CONSIDERAÇÕES FINAIS

O objetivo do estudo foi analisar o impacto e os potenciais desdobramentos da LGPD no meio corporativo. De caráter exploratório e descritivo a pesquisa procurou salientar os desafios trazidos pela nova lei. Devido a carência de estudos nacionais relacionados ao tema, utilizou-se uma abordagem bibliográfica contemplando artigos recentes de 2014-2020. Somando-se a isto, outras fontes secundárias foram empregadas para complementar a pesquisa (*sites* eletrônicos, livros, pesquisas de empresas de consultoria).

O estudo também apontou para os desafios, sem, no entanto, olvidar de mencionar os benefícios existentes para as empresas no tocante a implementação da Lei Geral de Proteção de Dados Pessoais. Vale destacar que apesar dos inúmeros obstáculos, as companhias que adotarem a nova lei se destacarão no cenário competitivo atual. Há que se observar que a LGPD não deve ser enxergada como ‘investimento ou custo’ para as organizações, pois esta representa um diferencial competitivo assim como indica comprometimento com as demandas da sociedade.

Do ponto de vista pragmático, conforme aponta Half (2019), há caminhos estratégicos para serem implementados de modo que se vença os obstáculos na implementação e conformidade com a LGPD nas empresas. Apesar disso, é fundamental analisar que cada empresa possui sua própria peculiaridade, isto é, empresas de pequeno e médio porte, que representam a maioria das empresas brasileiras, possuem impasses e vantagens próprios, diferentemente das empresas multinacionais ou nacionais de grande porte.

De fato, as empresas brasileiras, como analisado no estudo, não se encontram preparadas para adequação à nova realidade legal, entretanto, o principal gargalo ao entrave da nova lei consiste na carência de mão-de-obra especializada em conformidade com a nova realidade. Há também outros entraves relacionados, sobretudo, investimentos em tecnologia, treinamento, processos administrativos, política e diretrizes de segurança, além de medidas de segurança da informação que contemplem os três níveis: físico, organizacional e tecnológico que necessitam integração.

As limitações do presente estudo abrem novas possibilidades e novos espaços de significados e ressignificações a respeito do papel da nova lei no contexto empresarial. Por se tratar de uma pesquisa exploratória de cunho bibliográfico e qualitativo novos caminhos e desenhos podem ser explorados.

Recomenda-se para futuras pesquisas, o emprego de entrevistas junto aos profissionais encarregados pelo tratamento de dados (DPO) a fim de traçar os desafios relacionados à nova profissão no Brasil. Sugere-se também, um estudo de caso contrastando a realidade de empresas de portes e modelos de negócios iguais, ou ainda, completamente distintos para saber o nível de afetação inerente a cada uma, por fim, e não menos importante, uma abordagem quantitativa pode enriquecer a compreensão dos custos envolvidos na implementação da nova lei contribuindo inclusive para visualizar se a LGPD afeta de maneira semelhante ou não para determinado tipo de segmento, modelo e porte empresarial.

REFERÊNCIAS

ARAUJO, Alexandra Rodrigues et al. **Saúde Móvel: desafios globais à proteção de dados pessoais sob a perspectiva do direito da União Europeia.** 2016.

BAUMAN, Zygmunt. **Modernidade e ambivalência**. Trad. de Marcus Antunes Penchel. Rio de Janeiro: Zahar, 1999.

BAUMAN, Z.; DONKIS, L. **Cegueira Moral: a perda da sensibilidade na modernidade líquida.** 1. Ed. – Rio de Janeiro: Zahar, 2014.

BAUMAN, Z.; LYON, D. **Vigilância líquida: diálogos com David Lyon**. Rio de Janeiro: Zahar, 2013.

BBCBrasil.com. **Autoridades alemãs fazem alerta contra boneca que pode ser hackeada para espionar crianças.** Disponível em: <https://www.bbc.com/portuguese/internacional-39007610>. Acessado em: 28 mar. 2019.

BENTHAM, Jeremy. **O panóptico**. Belo Horizonte: Autêntica, 2008.

BRASIL. **Constituição Federal de 1988**. Disponível em: https://www.senado.leg.br/atividade/const/con1988/con1988_15.12.2016/art_5_.asp. Acessado em: 27 ago. 2020.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709)**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acessado em: 27 ago. 2020.

BREAK. **Vantagens e desvantagens da lei geral de proteção de dados: lei geral de proteção de dados entra m vigor em agosto de 2020. Entenda como funciona e de que forma impacta o mercado publicitário**. Disponível em: <https://negocios.empresaspioneiras.com.br/break/noticias/NOT,0,0,1462074,vantagens+e+desvantagens+da+lei+geral+de+protecao+de+dados.aspx#>. Acessado em: 12 out. 2020.

CASTELLS, Manuel. **A sociedade em rede**. Trad. de Roneide Venâncio Majer. 8. ed. São Paulo: Paz e Terra, 2011.

DW. **Rede alemã de supermercados é acusada de espionar funcionários**. Disponível em: <https://www.dw.com/pt-br/rede-alem%C3%A3-de-supermercados-%C3%A9-acusada-de-espionar-funcion%C3%A1rios/a-3218032>. Acessado em: 26 ago. 2020.

FOUCAULT, M. **Vigiar e punir**. Trad. de Raquel Ramalhete. 25. ed. Petrópolis: Vozes, 2002.

FUCHS, C. **Como podemos definir vigilância?.** São Paulo: Revista Matrizes, 2011.

GERHARDT, T. E., & SILVEIRA, D. T. (Orgs). **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GORDON, L. A.; LOEB, M. P. **The economics of information security investment**. United Satates: ACM Transactions on Information and System Security, 2002.

HALF, Robert. **Lei geral de proteção de dados pessoais: entenda o que é e como afeta o seu negócio**. Disponivel em: <https://www.roberthalf.com.br/central-do-conhecimento/carreira-e-mercado/lgpd-lei-geral-de-protecao-de-dados>. Acessado em: 05 out. 2020.

HAN, Byung-Chul. **A sociedade da transparência**. Petrópolis: Vozes, ISBN 978-85-326-5567-7, 2017a. e-book.

HARARI, Y.N. **The world after coronavirus**. Financial Times, 2020. Disponível em: <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75>. Acessao em: 05 set. 2020.

HARARI, Y.N. **Homo Deus: uma breve história do amanhã**. Rio de Janeiro: Companhia das Letras, 2016.

JENKINS, H. **A cultura da convergência**. São Paulo: Aleph, 2009.

KANT, Immanuel. **Fundamentação da metafísica dos costumes**. São Paulo: Abril, 1974.

LEE, Kai-Fu. **AI superpowers: China, Silicon Valley, and the new world order**. New York: Houghton Mifflin Harcourt, 2018.

LYON, D. **The culture of surveillance: watching as a way of life**. Cambridge: Polity, 2018.

LYON, D. **Surveillance society: monitoring everyday life**. Buckingham: Open University Press. 2001.

MARX, G. T. **Surveillance.** In Encyclopedia of privacy. (ed.). STAPLES, William G.535-544. Westport, CN: Greenwood Press, 2007.

MARX, Karl. **Manuscritos econômico-filosóficos**. Tradução de Jesus Ranieri. São Paulo: Boitempo, 2004.

NORRIS, C.; ARMSTRONG, G. **The maximum surveillance sociey: the rise of CCTV**. Oxford: Berg, 1999.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos. Paris: Artigo 12, 1948**. Disponível em: <https://nacoesunidas.org/artigo-12-direito-a-privacidade/>. Acessado em: 27 ago. 2020.

ORWELL, Geroge. **1984**. São Paulo: Cia das letras, 2009.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR – Lei nº 2016/679)**. Disponível em: <https://gdprinfo.eu>. Acessado em: 29.ago. 2020.

RAMONET, Ignácio. **O poder midiático**. In: MORAES, Denis (Org.). Por uma outra comunicação. Rio de Janeiro: Record, 2003.

ROLFINI, F. **Brasil teve mais de 1,6 bilhões de ataques cibernéticos em três meses: dados da Fortinet inidcam tentativas de invasão o primeio trimestre do ano, de um total de 9,7 bilhões na América Latina.** Olha digital, 2020. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/brasil-teve-mais-de-1-6-bilhao-de-ataques-ciberneticos-em-tres-meses/100420.> Acessado em: 30 ago. 2020.

SANTINO, R. **Google inclui microfone "secreto" em produto doméstico e não avisou usuários**. Olhar digital, 2019. Disponível em: <https://olhardigital.com.br/fique_seguro/noticia/google-incluiu-microfone-secreto-em-produto-domestico-e-nao-avisou-usuarios/83026>. Acessado em 26 ago. 2020.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2014.

TOFFLER, Alvin. **Powershift: as mudanças do poder**. Rio de Janeiro: Record, 2003.

VASARHELYI, M.A.; MOCK, T.J. **Sistemas de informação para administração**. Rio de Janeiro: Revista Administração de Empresas, 1974.

VERGARA, S.C. **Projetos e relatórios de pesquisa em administração**. ed.11. São Paulo: Atlas, 2009.

WOLF, Gary. **O eu quantificado**. TED Talks Cannes: jun. 2010. Disponível em: <https://www.ted.com/talks/gary_wolf_the_quantified_self?language=pt-br>. Acessado em: 28 ago. 2020.

ZUBOFF. S. **The age of surveillance capitalism: The fight for a human future at the new frontier of power**. New Yok: PublicAffairs, 2019.

ZUREIK, Elia. **Theorizing surveillance. The case of the workplace**. New York: Routledge, 2003.

Autoria:

Roger Luz da Rocha
Doutorando em Administração pelo Instituto de Pós-Graduação e Pesquisa em Administração da Universidade Federal do Rio de Janeiro - COPPEAD/UFRJ. Mestre em Administração pela Fundação Getúlio Vargas- EBAPE /RJ. Graduação em Administração pela Universidade Federal Rural do Rio de Janeiro, Pós-graduação em Marketing pelo Instituto Brasileiro de Mercado de Capitais IBMEC-RJ. Possui interesse nos seguintes temas: privacidade, proteção de dados, sistema de gestão de proteção de dados, gestão de riscos, segurança da informação, cybersecurity, governança de dados, sistemas de informação.
Instituição: UFRJ
E-mail: roger.ldr@gmail.com
Orcid: https://orcid.org/0000-0001-7261-101X
País: Brasil

Selma Velozo Fontes
Breve currículo
Professora da Universidade Federal Rural do Rio de Janeiro, Coordenadora de Disciplina na UAB/CEDERJ. Possui Bacharelado em Administração e Contabilidade, Licenciatura em Matemática, Especialização em Finanças Corporativas, Especialização em Planejamento, Implementação e Gestão em EAD, Especialização em Economia Comportamental, Mestrado em Gestão e Estratégia de Negócios e Doutorado em Ciências Empresariais e Sociais.
Instituição: UFRRJ
E-mail: svfontes@ufrrj.br
Orcid: https://orcid.org/0000-0001-8195-4823
País: Brasil

Thiago Fontes Machado
Estudante do curso de Direito na Universidade Federal do Estado do Rio de Janeiro - UNIRIO. Bolsista no grupo de pesquisa Poder e Território - Empoderamento local e ordenação Territorial. Realizou estágio na Defensoria Pública do Estado do Rio de Janeiro, no Núcleo de Atendimento à Pessoa com Deficiência - NUPED. Atualmente é estagiário da 3ª Vara Cível da Regional da Barra da Tijuca.
Instituição: UNIRIO
E-mail: thiago.machado@edu.unirio.br
Orcid: https://orcid.org/0009-0005-1421-4936
País: Brasil