Revista Direitos Sociais e Políticas Públicas Unifafibe

PONTOS CRÍTICOS PARA O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

CRITICAL POINTS OF PERSONAL DATA PROCESSING BY THE PUBLIC AUTHORITIES

Recebido em	23/07/2024
Aprovado em:	11/03/2025

Núbia Augusto de Sousa Rocha[1]
Alexandre Nascimento de Almeida[2]

RESUMO

O tratamento de dados pessoais pelo poder público vem sendo marcado por uma tensão entre o desenvolvimento de políticas públicas e a proteção de dados pessoais. A literatura sobre o tema se concentra majoritariamente no campo do Direito, com pouca discussão aplicada à Administração Pública. O objetivo deste artigo é identificar os pontos críticos para o tratamento de dados pessoais pelo poder público. Realizou-se uma revisão sistemática da literatura a partir do Methodi Ordinatio. Os principais pontos críticos foram: 1) a confiança dos cidadãos no Estado; 2) o grau de transparência das informações disponibilizadas pelo Estado; 3) os mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados; 4) a conformidade das instituições públicas com a legislação; 5) o interesse público motivador do tratamento dos dados; 6) e os desafios relacionados ao acesso à informação. Nesse sentido, a contribuição do presente estudo consiste no levantamento e análise dos estudos científicos acerca dos pontos críticos identificados possibilitando um maior conhecimento para a tomada de decisão do gestor público diante da tensão abordada.

Palavras-chave: Proteção de Dados Pessoas. Digitalização de Serviços Públicos. Governo Eletrônico. Governança de Dados.

[1] Graduação em Matemática pela Universidade de Brasília, mestre em Gestão de Políticas Públicas pelo Universidade de Brasília. Gestora da Telebras.
[2] Doutor. Professor da Universidade de Brasília (UnB) e orientador dos programas de Pós-graduação em Gestão Pública, Ciências Ambientais e Gestão e Regulação de Recursos Hídricos da Faculdade UnB de Planaltina.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

ABSTRACT

The processing of personal data by State has been marked by the tension that reflects the challenge of balancing the public policies development with protection of citizens' data. The literature on the subject is mostly concentrated in the field of Law, with little discussion applied to Public Administration. The paper objective is to identify the critical points for the processing of personal data by the State. A systematic review of the literature was carried out based on the Methodi Ordinatio. The main critical points were: 1) citizens' trust in the State for the processing of their data; 2) the degree of transparency of the information available by the State; 3) information security mechanisms and safeguards that guarantee the protection of data; 4) compliance of public institutions with legislation; 5) the public interest motivating the processing of data; 6) and the challenges related to access to information. In this sense, the contribution of this study consists of the survey and analysis of scientific studies on the identified critical points, enabling greater knowledge for the public manager's decision-making in the face of the tension addressed.

Keywords: Personal Data Protection. Digitalization of Public Services. Electronic Government. Data Governance.

INTRODUÇÃO

Os dados pessoais tornaram-se um dos recursos mais valiosos na sociedade da informação (FÉLIX; MONTEIRO, 2022). Nesse cenário, assim como as organizações do setor privado, as instituições do setor público investem cada vez mais recursos para alcançar os benefícios previstos da coleta e análise de dados para a prestação de serviços públicos, a exemplo dos custos aparentemente mais baixos, melhor eficiência na produção de serviços, previsão e antecipação da demanda por serviços e desenvolvimento de intervenções direcionadas (CHOROSZEWICZ; MÄIHÄNIEMI, 2020).

Como sublinham Teixeira e Guerreiro (2022), o poder público é um dos grandes agentes de tratamento de dados, devido ao seu papel no planejamento e execução de políticas públicas. Ressalta-se o contexto atual em que se observa maiores esforços de um governo eletrônico e um aumento contínuo das aplicações de Tecnologia da Informação e Comunicação – TIC no setor público. No Brasil, o Decreto 10.332, de 28 de abril de 2020, que institui a estratégia de governo digital (BRASIL, 2020), estabelece objetivos voltados

Revista | Direitos Sociais e Políticas Públicas Unifafibe

à integração de sistemas de informação do governo, bem como o fomento à interoperabilidade de sistemas e a oferta de serviços consolidados em plataforma única.

Bioni (2021) destaca que a relação entre o poder público e os titulares de dados pessoais é notada pela assimetria entre os atores, uma vez que o Estado é visto como detentor de posição de superioridade, e o interesse público tende a prevalecer quando em conflito com o interesse do indivíduo. Para Bellamy, Perry e Raab (2005), a tensão entre os objetivos de serviços públicos que exigem um compartilhamento de dados mais amplo e a proteção da privacidade representa um grande desafio para os formuladores de políticas públicas, reguladores e agentes de serviços públicos.

Logo, diante do contexto apresentado, a problemática do presente estudo centra-se no seguinte questionamento: quais os principais pontos de tensão para o tratamento de dados pessoais pelo poder público? Assim, delimitou-se o objetivo em identificar os principais pontos críticos para o tratamento de dados pessoais pelo poder público. Contribuindo para justificar a pesquisa, Rocha *et al*. (2023, p. 1) destacaram um "aumento significativo da produção acadêmica sobre o tema" nas últimas décadas, porém concentradas na área do direito, assim recomendaram o "desenvolvimento de mais pesquisas voltadas para o campo da Administração Pública".

1. FUNDAMENTOS TEÓRICOS

No Brasil, o tratamento de dados pessoais é regulamentado pela Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais – LGPD, que dispõe sobre as operações envolvendo dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (BRASIL, 2018) e constitui a principal parte do marco legal brasileiro em relação à coleta, ao armazenamento e ao uso de dados pessoais (OCDE, 2020).

Destaca-se que o objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018). Nesse contexto, Flôres e Silva (2020) evidenciam que a LGPD não torna impossível gerir dados, tampouco oferece riscos à inovação. Pelo contrário, ela promove e determina

Revista | Direitos Sociais e Políticas Públicas Unifafibe

mecanismos de controle e proteção do núcleo duro dos direitos fundamentais dos indivíduos.

Outro aspecto relevante sobre a LGPD é de que ela estabeleceu no ordenamento jurídico nacional o conceito de tratamento de dados pessoais, qual seja, toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Botelho (2020) evidencia que o tratamento de dados, conforme disposto na LGPD, abrange todo o ciclo de vida do dado, desde a sua coleta até a sua eliminação, ou ainda, nas palavras de Vainzof (2019, p. 116) "o conceito de tratamento abarca absolutamente todas as hipóteses de manuseio de dados".

Para que o tratamento de dados pessoais seja considerado adequado deve-se estabelecer controles administrativos, técnicos e físicos necessários à proteção da confidencialidade, integridade e disponibilidade dos ativos de informação em conformidade com as normas técnicas voltadas à segurança da informação, além da adequação às exigências da LGPD (HINTZBERGEN *et al.*, 2018), sobretudo porque a maneira como se dá o tratamento de dados pessoais pode afetar diretamente o direito à privacidade de qualquer indivíduo (ALVAREZ; TAVARES, 2017).

Oliveira e Araújo (2020) afirmam que o tratamento de dados pessoais é hoje uma realidade tanto no setor público como no privado, especialmente graças ao avanço das tecnologias de informação e comunicação, tão difundidas pela internet, por meio da qual pessoas, entidades e organizações compartilham informações cotidianamente.

Assim, considerando a relevância da questão, a LGPD estabeleceu, em seu artigo 7°, um rol taxativo de hipóteses em que é permitido o tratamento de dados pessoais, tais como o consentimento pelo titular de dados, o cumprimento de obrigação legal, dentre outras (BRASIL, 2018). Importa para o escopo deste trabalho ressaltar que uma das hipóteses previstas para o tratamento de dados pessoais permitidas pela LGPD se refere à execução de políticas pela administração pública:

Revista | Direitos Sociais e Políticas Públicas Unifafibe

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> [...] III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; (BRASIL, 2018).

Stelzer *et al*. (2019) pontuam que o dado pessoal é ativo importante para a concretização de políticas públicas. Nesse sentido, o acesso à informação se tornou indispensável para o próprio poder público que realiza a coleta dos mais diversos dados os quais podem ser de interesse para a gestão pública (FLÔRES; SILVA, 2020).

Entretanto, observa-se que o tratamento de dados pessoais pelo poder público possui muitas peculiaridades, em virtude da necessidade de compatibilizar o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na LGPD. Oliveira e Araújo (2020) ressaltam que a grande preocupação reside em como os dados pessoais estão sendo tratados, compartilhados e armazenados. Segundo os autores, cabe aos entes públicos garantir que, no estabelecimento de políticas públicas, a eficiência da coleta, do tratamento, do uso, do monitoramento, do armazenamento e do compartilhamento de dados pessoais sejam realizados com o menor risco à privacidade dos seus titulares e, por conseguinte, do cidadão.

Wimmer (2021) destaca que não é novidade e nem exclusividade do Brasil as preocupações quanto ao tratamento de dados pessoais de posse do poder público, em especial quando utilizados para finalidade distinta daquela que justificou a sua coleta inicial. Ainda em 1974, uma Resolução do Conselho da Europa relacionava a proteção da privacidade de indivíduos frente a bases de dados eletrônicas no setor público.

Sob este aspecto, o tratamento de dados pessoais pelo poder público revela uma dicotomia já apontada por Taylor, Lips e Organ (2008), na qual, de um lado, encontram-se os estudos sobre o tema que apresentam críticas à ampla captura e tratamento de dados pessoais pelo Estado e, do outro, os estudos na área de Administração Pública que se posicionam favoráveis a essa prática.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Em suma, embora o poder público tenha em seu favor exceções trazidas pela própria LGPD no âmbito do tratamento dos dados pessoais, que se justificam no princípio administrativo basilar da supremacia do interesse público sobre o privado (OLIVEIRA; ARAÚJO, 2020), existem questões críticas para o tratamento de dados pessoais pelo poder público. Nesse sentido, o desafio do Estado reside em "assegurar a celeridade e a eficiência necessárias à execução de políticas e à prestação de serviços públicos com respeito aos direitos à proteção de dados pessoais e à privacidade" (ANPD, p. 5, 2023).

2. PROCEDIMENTOS METODOLÓGICOS

A metodologia empregada nesta pesquisa é dedutiva, de natureza exploratória, apresenta uma abordagem qualitativa e teve como base uma revisão sistemática da literatura. Para Soares, Picolli e Casagrande (2018) essa metodologia de pesquisa se refere à uma investigação cientifica pautada por uma abordagem preestabelecida para selecionar, comparar e sintetizar as evidências sobre o assunto de interesse.

Neste estudo, a revisão sistemática foi realizada a partir do *Methodi Ordinatio*, método que conduz a busca, seleção e análise de artigos científicos, considerando a relevância das publicações e utiliza como critérios o número de citações, o fator de impacto e o ano de publicação dos estudos (PAGANI; KOVALESKI; RESENDE, 2015).

Para a busca dos artigos relacionados foram estabelecidas as seguintes palavras-chave: em português, "dados pessoais", "Poder Público", "Estado" e "Setor Público"; em inglês, "*Data Protection*" e "*Public Sector*". Foram utilizados os operadores booleanos *OR* e *AND* para investigar a relação entre os termos apresentados nos artigos.

Os bancos de dados selecionados para a busca foram o Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES e o *Scopus*. A escolha das plataformas de pesquisa se justifica por reunirem, em um único banco, diversas bases de dados, tais como a *Web of Science* e a *Science Direct*, o que resulta em uma consulta mais ampla.

A pesquisa nas bases de dados, realizada em agosto de 2022, contou apenas com artigos revisados por pares, com o objetivo de garantir maior confiabilidade dos estudos

Revista | Direitos Sociais e Políticas Públicas Unifafibe

selecionados. Além disso, não foi imposta nenhuma restrição quanto ao idioma da publicação e não foi estabelecido nenhum limite de ano de publicação para a pesquisa.

A consulta preliminar, segundo os critérios acima estabelecidos, retornou 173 artigos. O material passou por análise e filtragem, sendo eliminados os artigos repetidos, aqueles cujos assuntos não estavam relacionados ao tema e os que não foram possíveis localizar o texto integral. Ao fim, 43 artigos científicos foram selecionados para leitura sistemática e contribuíram para os resultados da pesquisa.

Na análise dos artigos selecionados foi empregada a técnica da análise de conteúdo para identificação dos pontos críticos para o tratamento de dados pessoais pelo poder público. A técnica tem por objetivo "compreender criticamente o sentido das comunicações, seu conteúdo manifesto ou latente, as significações explícitas ou ocultas" (CHIZZOTTI 2006, p. 98). Ademais, na visão de Flick (2009, p. 291), "a análise de conteúdo é um dos procedimentos clássicos para a análise de materiais textuais".

Importa destacar que, durante a leitura do portfólio selecionado, buscou-se identificar ainda outros trabalhos relevantes por meio da análise das referências utilizadas nos artigos selecionados, sendo possível detectar ainda outros trabalhos relacionados ao tema de forma assistemática em razão do conteúdo apresentado.

3. RESULTADOS E DISCUSSÃO

Da análise do portfólio bibliográfico selecionado, identificou-se que seis foram os pontos críticos mais destacados na literatura: 1) a confiança dos cidadãos no Estado para o tratamento de seus dados pessoais; 2) o grau de transparência das informações disponibilizadas pelo Estado no que se refere ao tratamento dos dados pessoais do cidadão; 3) os mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado; 4) a conformidade das instituições públicas com a legislação sobre o tema; 5) o interesse público motivador do tratamento dos dados; 6) e os desafios relacionados ao acesso à informação. A Tabela 1 demonstra a proporção de artigos que abordam os pontos de tensão identificados em relação ao total do portfólio selecionado.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Tabela 1. Distribuição dos pontos críticos observados no portfólio

Ponto Crítico	Percentual de artigos que abordam o assunto
Confiança	21%
Transparência	26%
Segurança	21%
Conformidade	12%
Interesse Público	30%
Acesso à Informação	7%

Fonte: Elaborado pelos autores

Depreende-se da Tabela 1 que o interesse público foi o assunto mais observado, sendo que 30% dos artigos que compõe o portfólio abordam direta ou indiretamente o assunto. Já o acesso à informação foi o menos frequente, sendo tratado em apenas 7% dos estudos selecionados.

Registra-se que, de forma residual, a literatura sobre o tema também cita outros pontos críticos, tais como o emprego de tecnologias emergentes (inteligência artificial, aprendizado de máquina, robótica e *big data*) e a potencial discriminação algorítmica (SARABDEEN; CHIKHAOUI; ISHAK, 2022). Entretanto, não foram identificados estudos que abordassem tais assuntos com profundidade no portfólio bibliográfico selecionado.

3.1 Confiança

A literatura analisada aponta que a confiança da sociedade no Estado é um ponto crítico para a implementação de políticas públicas que exijam o tratamento de dados pessoais pelo poder público. Os processos de digitalização no setor público levaram a um aumento de abordagens inovadoras para uma melhor prestação de serviços usando TICs. Os cidadãos, no entanto, muitas vezes guardam reservas em relação aos esforços de governo eletrônico devido a preocupações com a proteção de dados (PLEGER; GUIRGUIS; MERTES, 2021).

Ainda em 2005, Lips, Taylor e Bannister (2005) já apontavam que a confiança deve ser reconhecida como um dos conceitos centrais nas ambições dos governos para lidar com a sociedade da informação. Nesta esteira, Combe (2009) argumenta que a efetiva

Revista | Direitos Sociais e Políticas Públicas Unifafibe

prestação de serviços públicos por meio das TICs depende necessariamente de relações de confiança entre os cidadãos e o Estado.

Corroboram com este entendimento Pleger, Guirguis e Mertes (2021), segundo os quais a confiança é de particular importância no contexto da administração pública e da implementação de serviços eletrônicos do governo. Isto porque, para que os usuários estejam dispostos a fornecer informações pessoais *online*, eles devem ter confiança de que seus dados não serão usados de forma indevida (LANDWEHR, 2019).

Para Perry, Raab e Bellamy (2005) as práticas eficazes de proteção de dados são amplamente consideradas como condição necessária para construir a confiança popular nos serviços eletrônicos fornecidos pelo Estado e, portanto, como uma fonte significativa de vantagem competitiva na economia eletrônica global.

Países como o Reino Unido e a Índia, em que pese nutram boas intenções ao implementar sistemas que necessitam do tratamento de dados pessoais pelo poder público – a exemplo de Identidades Digitais –, na visão de Sule, Zennato e Thomas (2021), falharam em função da falta de confiança do usuário.

Segundo Sarabdeen, Chikhaoui e Ishak (2022), a perda de confiança do público para com os mecanismos de proteção de dados adotados pelo governo pode ser ainda mais grave em tempos de crise, – a exemplo da Pandemia de Coronavírus, em que diversos países disponibilizaram bancos de dados de saúde para ampla reutilização e tratamento diverso daqueles que haviam motivado sua coleta e uso original.

Almeida *et al*. (2020) entendem que, para ampliar a confiança dos indivíduos e da sociedade na utilização de seus dados, ainda que para responder a situações de legítimo interesse público, há de se estabelecer modelos de governança de dados mais justos, responsáveis e sustentáveis, que protejam e defendam princípios éticos e regulatórios, em especial quando se trata de dados pessoais compartilhados entre o setor público e o privado.

Nesse sentido, destaca-se o argumento de Black e Stevens (2013) de que, quando o Estado preza pela confiança do cidadão no tratamento de seus dados pessoais, os

Revista | Direitos Sociais e Políticas Públicas Unifafibe

indivíduos sentem que seus direitos estão sendo tratados com respeito o que leva ao desenvolvimento de uma cultura de proteção de dados mais robusta no setor público.

3.2 Transparência

A transparência das operações utilizando dados pessoais pelo Estado é primordial para a sociedade informacional, pois proporciona ao cidadão o acesso a suas informações e contribui para que o indivíduo possa acompanhar a administração de seus dados. Nesse sentido, ainda que estejam sendo utilizados para finalidade de interesse público, os dados compõem a personalidade do titular e requerem mecanismos efetivos de proteção (FÉLIX; MONTEIRO, 2022).

Cumpre registrar que a legislação brasileira prevê que o poder público deverá informar de maneira clara, transparente e acessível as hipóteses em que se realiza o tratamento de dados pessoais, bem como sua finalidade, os procedimentos adotados e as práticas utilizadas para tanto (MACIEL, 2020).

Para Almeida *et al.* (2020), ao considerar que dados podem ser utilizados e compartilhados por diferentes pessoas e organizações simultaneamente, as questões principais a serem harmonizadas giram em torno da governança responsável dos dados baseada na transparência para que se estabeleça um relacionamento equilibrado e justo entre indivíduos e organizações. Os autores reforçam ainda que dados coletados, compartilhados e utilizados em prol da execução de políticas públicas, a exemplo da saúde, precisam apresentar termos e condições claros e transparentes sobre os propósitos de acesso, compartilhamento, usos e responsabilidades.

Corroboram com este entendimento Modesto e Ehrhardt Junior (2020), segundo os quais os dados pessoais são extensão dos direitos de personalidade da pessoa natural, devendo-se garantir aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (responsáveis pela coleta e utilização dos dados), como expressão da transparência que deve ser mantida em operações deste tipo.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Segundo Pleger, Guirguis e Mertes (2021), o Estado é visto pelo cidadão como responsável por garantir a proteção de dados. Nesse sentido, ao exigir que o Estado forneça informações transparentes aos seus cidadãos, no que se refere ao tratamento de seus dados pessoais, uma questão importante deve ser abordada: a informação deve ser apropriada ao grupo-alvo para atender adequadamente às suas preocupações e o discurso público deve levar isso em conta.

Os autores argumentam ainda que a transparência também requer o envolvimento ativo do público e, portanto, os cidadãos precisam ser proativos em se informar. Nesse sentido, os autores incentivam os governos a dialogar com os cidadãos para melhor compreender sua perspectiva subjetiva em termos de proteção de dados e aumentar a transparência, de maneira compreensível, sobre como seus dados estão sendo utilizados.

O problema passa a residir quando o Estado deixa de ser transparente nas suas informações sobre o tratamento dos dados dos seus cidadãos. Segundo Palhares *et al*. (2020), diversos países vêm experimentando críticas quanto às medidas adotadas no tratamento de dados pessoais para atendimento de políticas públicas, sobretudo quando há falta de transparência e falta de diálogo com a população.

Percebe-se na literatura analisada que mecanismos garantidores da transparência no tratamento de dados pessoais pelo poder público podem atenuar os impactos da falta de confiança do cidadão, abordados na seção anterior. Segundo Martins *et al.* (2020), quanto mais transparência, mais confiança a sociedade tem na informação e, portanto, maior é a adesão esperada nas medidas implementadas pelo Estado.

Para Félix e Monteiro (2022) o tratamento de dados pessoais é necessário para elaboração e implementação de políticas públicas. Nesse sentido, não cabe questionar se o tratamento deve ou não ocorrer, mas sim debater como fazê-lo de forma eficiente e de modo a incorrer em menos riscos para os cidadãos. Os autores concluem que a transparência é o caminho para que a própria população ativamente desempenhe seu papel social.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

3.3 Segurança

Para Phillips (2021), a ocorrência de uma violação de dados pessoais é outra parte crítica da legislação de proteção de dados. Segundo o autor, apesar das organizações adotarem salvaguardas e medidas de mitigação por meio de políticas e técnicas de segurança, é inevitável que alguém manipule dados pessoais incorretamente ou ainda que criminosos cibernéticos ameacem a proteção de dados pessoais.

Este ponto também é abordado por Naarttijärvi (2018), segundo o qual a falta de segurança da informação implica em deficiências na proteção de dados armazenados em sistemas públicos de informação. Perry, Raab e Bellamy (2005) corroboram com esse entendimento, ao destacarem que a segurança assume especial relevância quando se trata do compartilhamento de dados pessoais pelos governos. Sendo assim, o uso compartilhado ou outros tipos de tratamento de dados pessoais pela Administração Pública requer mecanismos e ferramentas que garantam a segurança da informação, a partir de medidas técnicas em que a proteção desses dados seja minimamente garantida (OLIVEIRA; ARAÚJO, 2020).

Na visão de Flôres e Silva (2020), a concessão dos dados por parte do cidadão confere grande responsabilidade ao ente público em armazená-los de forma segura, o que nem sempre acontece. Van Slyke *et al.* (2006) aponta que os governos vêm sendo questionados por negligenciar as salvaguardas apropriadas na coleta de dados ou de não investir o suficiente na proteção desses dados.

Fato é que, ultimamente, violações de dados e roubos de identidade em grande escala tem se tornado cada vez mais comuns em todo o mundo (SULE; ZENNATO; THOMAS, 2021). Nesse sentido, Black e Stevens (2013) apontam que a imprensa de alto perfil vem relatando as violações graves de proteção de dados por organizações do setor público, geralmente envolvendo a perda de dados pessoais por meio de práticas inadequadas de manipulação e retenção de dados.

Em abril de 2020, a CNN (2020) reportou uma onda crescente de ataques cibernéticos a agências governamentais e instituições médicas dos EUA que lideravam a resposta à pandemia de coronavírus por grupos criminosos. Em junho de 2020, o

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Primeiro-Ministro australiano admitiu que as atividades maliciosas cresceram ao longo dos meses, embora nenhuma grande violação de dados pessoais tenha sido registrada (BBC, 2020).

No Brasil, o cenário não é diferente. Em dezembro de 2021, foi noticiado que uma falha de segurança no Ministério da Saúde havia exposto os dados pessoais de mais de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde – SUS (ESTADÃO, 2020).

Por consequência, a literatura aponta uma convergência para o entendimento sintetizado por Mikkelsen *et al.* (2020), segundo o qual os dados devem ser suficientemente protegidos tanto tecnicamente contra riscos cibernéticos quanto organizacionalmente contra o compartilhamento não-autorizado. Entretanto, o cenário apresentado acima indica que ainda é um desafio para o Estado a defesa da proteção de dados pessoais por meio de medidas de segurança suficientes.

3.4 Conformidade

O grau de conformidade, ou de ausência dela, com a legislação sobre o tema também foi um fator apontado recorrentemente nos artigos selecionados. Para Chua *et al*. (2017), as organizações governamentais devem ser as líderes no cumprimento da regulação estipulada para reger os processos negociais e defender as leis e ordens a nível nacional. Na visão dos autores, o Estado deve servir de modelo para convencimento das organizações não-governamentais de que a conformidade com a legislação deve ser levada a sério.

Sob esse aspecto, a criticidade reside no sentido de que a literatura investigada aponta que, em diversos países, o setor público não está aderente às imposições da legislação para garantia da proteção de dados pessoais. Um estudo realizado na Malásia investigou o grau de conformidade das organizações quanto à sua legislação de proteção de dados pessoais e apontou que as organizações governamentais do país têm pontuação de conformidade inferior quando comparadas as organizações não-governamentais (CHUA *et al*., 2017).

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Black e Stevens (2013) relatam que uma auditoria realizada entre fevereiro de 2010 e julho de 2012 pelo *Information Commissioner's Office* – ICO, autoridade de proteção de dados pessoais do Reino Unido, investigou organizações do setor público e privado quanto à conformidade geral com a legislação aplicável. O resultado da auditoria demonstrou que os órgãos públicos, via de regra, apresentam registros de conformidade insatisfatórios, especialmente quando comparados a organizações do setor privado. Como consequência, o ICO impôs multas fiduciárias a vinte diferentes órgãos do setor público por violações de proteção de dados, em contraste marcante com as penalidades aplicadas contra apenas três empresas privadas.

Em um estudo realizado na Dinamarca, Blume (2012) revela que em certos casos, a exemplo dos prazos para armazenamento e eliminação de dados pessoais, a tradição administrativa prevaleceu e, em muitos aspectos, a prática seguida pelas autoridades públicas não está em total conformidade com a legislação do país.

Mais um exemplo se dá em um estudo de caso que analisou a deliberação da Comissão Nacional de Proteção de Dados – CNPD no âmbito de processo de investigação e inquérito contra a Autoridade Tributária de Portugal (CORREIA; JESUS; PEREIRA, 2019). A Comissão concluiu que o tratamento de dados pessoais realizado pelo órgão público não estava em conformidade com a lei, recomendando diversos procedimentos para que fossem atendidas as imposições legais.

No Brasil, o cenário não se revelou diferente. No primeiro trimestre de 2021, o Tribunal de Contas da União – TCU realizou auditoria que buscou avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. O Tribunal concluiu que 55% dos Órgãos não haviam sequer conduzido iniciativas para identificar e planejar as medidas necessárias à adequação à normativa (TCU, 2022).

Assim, ao considerar que as autoridades públicas processam a maioria dos dados pessoais de uma população (BLUME, 2012), as consequências da desconformidade com a legislação aplicável podem ser inúmeras. Black e Stevens (2013) citam, como um exemplo,

Revista | Direitos Sociais e Políticas Públicas Unifafibe

que a falta de orientações sobre a conformidade do setor público no tratamento de dados pessoais pode resultar em uma falta de padronização entre as diferentes organizações deste setor. Como é o caso do Reino Unido, em que há práticas diversas, aumentando a desinformação e a falta de confiança em cada organização individual promove ainda mais uma cultura de cautela por parte dos cidadãos.

Percebe-se ainda que a não-adequação à legislação também está diretamente relacionada ao estabelecimento de um ambiente de mais ou menos confiança do cidadão no que se refere ao tratamento de seus dados pessoais pelo poder público. Segundo Sarabdeen, Chikhaoui e Ishak (2022), o cumprimento dos princípios para a proteção de dados pessoais permite construir a confiança da comunidade nas medidas governamentais e organizacionais, ainda que o processamento de dados esteja dentro das exceções permitidas pela legislação aplicável.

Nesse sentido, Chua *et al*. (2017), recomendam que o Estado deve rever sua estratégia de proporcionar um ambiente propício e mecanismos de monitoramento eficazes para avançar em direção a um nível mais alto de conformidade. Para Blume (2012) a falta de conformidade constatada no setor público se dá em grande medida em razão da legislação sobre o tema abranger tanto o setor público quanto o privado. Na visão de Blume (2012), uma regulamentação separada tornaria mais óbvio que a proteção de dados faz parte do Direito Administrativo, podendo ser redigida em melhor conformidade com outras regras administrativas e determinar com mais precisão como e em que medida os dados pessoais podem ser processados por este setor.

Wimmer (2021) destaca que a plena observância da LGPD pelo poder público requererá mudanças de cultura e de procedimentos, como por exemplo a incorporação da prática de elaboração de relatórios de impacto à proteção de dados pessoais antes da adoção de novos procedimentos, métodos e tecnologias, bem como a consideração de tais preocupações também quando da edição de atos normativos dotados de generalidade e abstração.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

3.5 Interesse Público

O interesse público deve ser o alicerce de qualquer operação de uso de dados pessoais, uma vez que, quando a Administração Pública atua no campo da privacidade e dos dados pessoais, o tratamento é um ato administrativo e, como tal, detém como pressuposto de validade a finalidade pública (OLIVEIRA; ARAÚJO, 2020).

Importa observar o que a legislação sobre o tema estabelece. O Regulamento Geral sobre a Proteção de Dados europeu definiu, em seu artigo 6°, que o tratamento de dados pessoais é legítimo para a execução de uma missão realizada no interesse público ou no exercício da autoridade oficial investida no controlador (CORREIA; JESUS; PEREIRA, 2019). No que se refere à legislação brasileira, a LGPD impôs, em seu artigo 23, às pessoas jurídicas de direito público a observância da finalidade pública, a persecução do interesse público, quando exercerem atividade de tratamento de dados pessoais (OLIVEIRA; ARAÚJO, 2020).

Nesse sentido, Maciel (2020) destaca que é necessário que a coleta de dados pessoais tenha como finalidade sua utilização para fins do interesse público, de modo que o seu resultado venha a ser revertido em proveito de toda a sociedade e para a melhoria dos serviços públicos. Com o objetivo de compreender como as Instituições de Ensino Superior – IES no Brasil podem adequar à LGPD no aspecto finalidade, Gomes, Filho e Luccas (2023) sugeriram a criação de quatro categorias de estudantes, permitindo o estabelecimento de um regime de proteção e de gestão de dados específico para cada categoria.

Assim, uma vez que a relação entre o Estado e seus cidadãos deriva de um processo contínuo, o tratamento dos dados pessoais deve ser baseado em justificativas que demonstrem que o processamento de seus dados se dará apenas quando estiver relacionado ao interesse público da sociedade como um todo (BLACK; STEVENS, 2013).

Considerando este aspecto, a tensão sobre o interesse público reside na delicada interação entre a proteção de dados pessoais, por um lado, e a prestação de serviços públicos, por outro (SARABDEEN; CHIKHAOUI; ISHAK, 2022).

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Para Black e Stevens (2013), é essencial examinar como os interesses concorrentes podem ser ponderados, sendo o interesse público o fator decisório. Na visão dos autores, a tentativa de equilibrar o interesse público com os direitos e liberdades fundamentais de um indivíduo é, por vezes, insatisfatória e desigual. Corroboram com esse entendimento Sarabdeen, Chikhaoui e Ishak (2022) ao afirmarem que o êxito das medidas de implementação para utilização de dados pessoais pelo poder público depende do equilíbrio entre o interesse público de usar os dados e o direito privado de proteger os mesmos dados.

Nesse sentido, Modesto e Ehrhardt Junior (2020) entendem que o estabelecimento do ponto de equilíbrio no tratamento dos dados pessoais em prol do interesse coletivo é tarefa bastante árdua, razão pela qual os limites precisam ser construídos na análise do caso concreto.

Perry, Raab e Bellamy (2005) destacam que os Estados têm frequentemente recorrido à noção de interesse público, justificando o tratamento de dados pessoais, por exemplo, para travar uma guerra contra o terrorismo, combater o crime ou proteger o erário público. Um contraponto a esse argumento é apresentado por Neto e Demoliner (2018) ao chamar atenção que, embora não se possa discordar que a tutela do Estado sobre a privacidade deve levar em conta as exigências da defesa nacional e pública, existe o risco de que, nas mãos de determinados agentes de segurança, a ponderação entre interesses igualmente tutelados seja desvirtuada de modo que, em nome da segurança nacional, seriam tolerados abusos dos mais diversos.

Wimmer (2021) ressalta que o uso e tratamento de dados pessoais pelo poder público tem sido historicamente polemizado a partir de duas linhas interpretativas distintas: de um lado, destacam-se os riscos associados à vigilância e ao controle da sociedade; de outro, a eficiência e a modernização do Estado. Sob esse aspecto, Bioni (2021) pondera que a privacidade deve ser encarada como um bem comum, o qual detém particular importância para o estado democrático de direito, uma vez que garante a participação deliberativa e heterogênea entre os cidadãos em contraste às sociedades totalitárias. A privacidade não beneficia, portanto, somente o indivíduo, mas,

Revista | Direitos Sociais e Políticas Públicas Unifafibe

colateralmente, a sociedade como um todo, revelando-se enquanto elemento constitutivo da própria vida em sociedade.

Assim, a criticidade sobre este elemento é reforçada ao constatar os aspectos contrapostos: embora o interesse público seja o cerne para o tratamento de dados pelo poder público, a privacidade e o direito à proteção de dados pessoais também são de interesse público, necessários inclusive para manutenção do Estado democrático de direito.

3.6 Acesso à Informação

Outro ponto crítico identificado na literatura é a conciliação do direito ao acesso à informação pública com a proteção de dados pessoais. Para Wimmer (2021), a aparente tensão entre publicidade e privacidade tem sido sublinhada no contexto da necessidade de conciliar regras que impõem ao Estado um alto grau de disponibilização de informações quanto às suas atividades com as que exigem que dados pessoais sejam tratados de maneira a preservar a sua intimidade, vida privada, honra e imagem.

Flôres e Silva (2020) defendem que um dos maiores desafios da Administração Pública no Brasil é atender às regras previstas na Lei de Acesso à Informação – LAI (BRASIL, 2011), frente às garantias estabelecidas na LGPD. Somam-se a esse entendimento Oliveira e Araújo (2020), segundo os quais aos gestores públicos incube um grande desafio de acomodar o acesso à informação, que deve reger os atos da Administração Pública, ao passo que observam o regime jurídico de proteção de dados pessoais.

Destaca-se que, para além de ser um direito de todos, o acesso à informação é essencial para as sociedades democráticas, uma vez que ao se manterem informados sobre as ações do Estado, a população adquire condições de exercer certo controle social (FLÔRES; SILVA, 2020). Entretanto, Gonçalves (2019) ressalta que ações da Administração Pública, ainda que bem-intencionadas, que visam ao atendimento do direito ao acesso à informação e do princípio da publicidade, também podem ferir os

Revista | Direitos Sociais e Políticas Públicas Unifafibe

direitos da personalidade ao permitir o acesso a terceiros ou tornar públicos dados pessoais.

A despeito dos argumentos apresentados até aqui, que colocam o acesso à informação como um desafio para a proteção de dados pessoais pelo poder público, Wimmer (2021, p. 271) entende que os dois direitos podem ser harmonizados. A autora sustenta que:

> Apesar de adotarem lógicas distintas e, inclusive, terminologias distintas, observa-se que tanto a LAI como a LGPD buscam materializar seus princípios orientadores de modo a construir uma narrativa que permita aliar a lógica de transparência e a lógica de proteção. A LAI, por exemplo, introduz a ideia de consentimento para viabilizar a divulgação de informações pessoais; a LGPD faz referência explícita à LAI para operacionalizar o exercício de direitos nela previstos perante o poder público; além disso, indica que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. A ideia de qualidade dos dados está presente em ambas as normas, assim como a preocupação com a segurança (WIMMER 2021, p. 271).

Nesse sentido, embora se constate um possível atrito entre privacidade e publicidade, quando as legislações sobre acesso à informação e proteção de dados pessoais são colocadas em perspectivas contrapostas, é possível buscar uma compatibilização entre as leis, na medida em que se verificam outras formas de disponibilizar o acesso à informação de maneira menos gravosa ao titular de dados pessoais (ANPD, 2023).

CONCLUSÕES

Este estudo buscou investigar os principais pontos críticos abordados pela literatura para o tratamento de dados pessoais pelo poder público, tendo como base uma revisão sistemática sobre o tema. Como resultado, foram identificados seis elementos de tensão destacados nos artigos analisados: confiança, transparência, conformidade, segurança, interesse público e acesso à informação.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

A literatura aponta que a confiança dos cidadãos no Estado para o tratamento de seus dados pessoais é elemento fundamental para implementação de políticas públicas, em especial no que se refere à digitalização de serviços e às iniciativas de governo eletrônico. Verificou-se ainda que outros pontos críticos identificados, tais como a segurança da informação e a transparência, podem afetar ainda mais a confiança do titular de dados nas ações do poder público.

O grau de transparência das informações disponibilizadas pelo Estado no que se refere ao tratamento dos dados pessoais do cidadão é também considerado um ponto de tensão pela literatura, pois quando o poder público deixa de fornecer informações claras, precisas e de fácil acesso sobre a guarda e o tratamento de dados pessoais, há uma afronta ao direito de personalidade da pessoa natural.

A literatura também aponta uma convergência para o entendimento de que o poder público deve se cercar de mecanismos de segurança da informação e salvaguardas que garantam a proteção dos dados pessoais em posse do Estado. Entretanto, verifica-se ser cada vez mais comum a prática de violações de dados e roubo de identidade em grande escala demonstrando que a segurança é um ponto crítico para o Estado quando da guarda e tratamento de dados pessoais.

Em que pese a sociedade atribuir ao Estado, enquanto ente regulador e garantidor da proteção de dados pessoais, o dever de ser exemplo de cumprimento das regras, com o intuito de propiciar o convencimento das organizações não governamentais de que a conformidade com a legislação deve ser seguida, a falta de conformidade das instituições públicas com a legislação sobre o tema foi identificada em estudos realizados em diversos países.

A doutrina destaca, ainda, o interesse público como principal motivador para o tratamento de dados pessoais pelo Estado. Todavia, faz-se necessária uma avaliação quanto ao seu uso indiscriminado sob o pretexto do bem coletivo, tendo em vista que a privacidade e o direito à proteção de dados pessoais também são de interesse público – necessários inclusive para manutenção do Estado democrático de direito – e devem ser observados a fim de se buscar um equilíbrio entre os dois horizontes da análise.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

Por fim, a literatura destaca ainda uma aparente tensão entre privacidade e publicidade, quando a legislação sobre acesso à informação e proteção de dados pessoais são colocados em perspectivas contrapostas. Entretanto, é possível vislumbrar uma harmonização entre as leis, na medida em que se verifique outras formas de disponibilizar o acesso à informação de maneira menos gravosa ao titular de dados pessoais.

Uma limitação ao desenvolvimento deste trabalho está relacionada ao desafio de identificação de referências bibliográficas aplicadas à Administração Pública. Assim, os pontos de tensão abordados por este estudo têm o potencial de embasar uma agenda de futuras pesquisas que permitam explorar com maior profundidade o referencial teórico de cada fator especificamente na área estudada, bem como suas implicações para o tratamento de dados pessoais pelo Poder Público.

Ademais, considerando a lacuna apresentada pela literatura, alguns órgãos governamentais têm emitido recomendações práticas para auxiliar a atuação dos gestores públicos na aplicação da LGPD, tais como um guia de boas práticas (SGD,2020) e outras orientações operacionais para adequação das instituições públicas à LGPD.

Diante do exposto, conclui-se que o tratamento de dados pessoais pelo poder público possui vários aspectos relevantes que impõem diversos desafios ao gestor público, que ao planejar, implementar e avaliar políticas públicas, deve considerar os pontos críticos abordados neste estudo.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo. *et al*. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva**, Rio de Janeiro, v. 25, n. 1, p. 2487-2492, 2020. DOI: https://doi.org/10.1590/1413-81232020256.1.11792020

ALVAREZ, Bruna Acosta; TAVARES, Letícia Antunes. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. *In*: ONODERA, Marcos Vinicius Kiyoshi; FILIPPO, Thiago Baldani Gomes de (Org.). **Brasil e EUA: temas de direito comparado**. São Paulo: Escola Paulista da Magistratura, 2017. p. 155-203.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

ANPD - Autoridade Nacional de Proteção de Dados. **Guia orientativo: Tratamento de dados pessoais pelo Poder Público.** Brasília, DF: ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em 15 jul. 2023.

BBC. **Australia cyber-attacks: PM Morrison warns of 'sophisticated' state Hack**, 2020. Disponível em: <https://www.bbc.com/news/world-australia-46096768>. Acesso em: 14 jul. 2023.

BELLAMY, Christine; PERRI, Six; RAAB, Charles. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part II. **Public administration**, v. 83, n. 2, p. 393-415, 2005. DOI: https://doi.org/10.1111/j.0033-3298.2005.00455.x

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3 ed. Rio de Janeiro: Editora Forense, 2021.

BLACK, Gillian; STEVENS, Leslie. Enhancing data protection and data processing in the public sector: The critical role of proportionality and the public interest. **SCRIPT-ed**, v. 10, n. 1, p. 93-122, 2013. DOI: https://doi.org/10.2966/scrip.100113.93

BLUME, Peter. The inherent contradictions in data protection law. **International data privacy law**, v. 2, n. 1, p. 26-34, 2012. DOI: https://doi.org/10.1093/idpl/ipr020

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista de Direitos Sociais e Políticas Públicas**, v. 8, n. 2, p. 197-231, 2020. DOI: https://doi.org/10.25245/rdspp.v8i2.705

BRASIL. **Lei n º 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação. Brasília, DF: Presidência da República, 2011.

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. **Decreto nº 10.332 de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022. Brasília, DF: Presidência da República, 2020.

CHIZZOTTI, Antônio. **Pesquisa qualitativa em ciências humanas e sociais**. São Paulo: Cortex, 2006.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

CHOROSZEWICZ, Marta; MÄIHÄNIEMI, Beata. Developing a digital welfare state: Data protection and the use of automated decision-making in the public sector across six EU countries. **Global Perspectives**, v. 1, n. 1, 2020. DOI: https://doi.org/10.1525/gp.2020.12910.

CHUA, Hui Na; HERBLAND, Anthony; WONG, Siew Fan; CHANG, Younghoon. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. **Telematics and informatics**, v. 34, n. 4, p. 157-170, 2017. DOI: https://doi.org/10.1016/j.tele.2017.01.008

CNN. **They are trying to steal everything**, 2020. US coronavirus response hit by foreign hackers. Disponível em: <https://edition.cnn.com/2020/04/25/politics/us-china-cyberattacks-coronavirus-research/index.html>. Acesso em: 14 jul. 2023.

COMBE, Colim. Observations on the UK transformational government strategy relative to citizen data sharing and privacy. **Transforming Government People Process and Policy**, v. 3, n. 4, p. 394-405, 2009. DOI: https://doi.org/10.1108/17506160910997892

CORREIA, Pedro Miguel Alves Ribeiro; JESUS, Inês Oliveira Andrade de; PEREIRA, Sandra Patrícia Marques. O tratamento de dados pessoais na administração pública portuguesa: o caso de estudo da opacidade da autoridade tributária. **Lex Humana**, v. 11, n. 2, p. 128-142, 2019.

ESTADÃO. **Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros**, 2020. Acesso em: <https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340>. Disponível em: 14 jul. 2023.

FÉLIX, Victória; MONTEIRO, Juliano Ralo. O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19. **civilistica.com**, v. 11, n. 1, p. 1-31, 2022.

FLICK, Uwe. **Introdução à pesquisa qualitativa**. São Paulo: Artmed, 2009.

FLÔRES, Mariana Rocha de; SILVA, Rosane Leal da. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. **Revista de direito**, v. 12, n. 2, p. 01-34, 2020. DOI: https://doi.org/10.32361/2020120210327

Revista | Direitos Sociais e Políticas Públicas Unifafibe

GOMES, Fabricio Vasconcelos; CUNHA FILHO, Marcelo Castro; LUCCAS, Victor Nóbrega. Proteção de dados e instituições de ensino: o que fazer com dados de alunos? **Revista Brasileira de Políticas Públicas**, v. 13, n. 1, p. 401-420, 2023. DOI: https://doi.org/10.5102/rbpp.v13i1.7996

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de dados pessoais e sensíveis pela administração pública federal: desafios, modelos e possíveis impactos com a nova lei**. Dissertação (Mestrado em Direito) – Centro Universitário de Brasília, Brasília, 2019.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.

LANDWEHR, Carl. 2018: A big year for privacy. **Communications of the ACM**, v. 62, n. 2, p. 20-22, 2019. DOI: https://doi.org/10.1145/3300224

LIPS, Miriam; TAYLOR, John. A.; BANNISTER, Frank. Public administration in the information society: Essays on risk and trust. **Information polity**, v. 10, n. 1, p. 1-9, 2005. DOI: https://doi.org/10.3233/IP-2005-0073

MACIEL, Moises. Os tribunais de contas no exercício do controle externo de acordo com nova Lei Geral de Proteção de Dados Pessoais. **Revista Controle: Doutrinas e artigos**, v. 18, n. 1, p. 20-45, 2020.

MARTINS, Helena; FERREIRA, Katiele Gomes; CASTRO, Luciana Gouvêa Hage de; MACÊDO JUNIOR, Daniel Paiva de; LIMA, Elizandro dos Anjos Araújo. Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará. **Liinc em revista**, v. 16, n. 2, p. e5387, 2020. DOI: https://doi.org/10.18617/liinc.v16i2.5387

MIKKELSEN, Daniel; SOLLER, Henning; STRANDELL-JANSSON, Malin. **Privacy, security, and public health in a pandemic year**, 2020. Disponível em: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/privacy-security-and-public-health-in-a-pandemic-year>. Acesso em: 14 jul. 2023.

MODESTO, Jéssica Andrade; EHRHARDT JUNIOR, Marcos. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. **Revista Eletrônica Direito e Sociedade - REDES**, v. 8, n. 2, p. 1-19, 2020. DOI: https://doi.org/10.18316/REDES.v8i2.6770

NAARTTIJÄRVI, Markus. Balancing data protection and privacy – The case of information security sensor systems. **Computer law & security review**, v. 34, n. 5, p. 1019-1038, 2018. DOI: https://doi.org/10.1016/j.clsr.2018.04.006

Revista | Direitos Sociais e Políticas Públicas Unifafibe

NETO, Eugênio Facchini; DEMOLINER, Karine Silva. Direito à privacidade e novas tecnologias: Breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. **Revista internacional Consinter de direito**, v. 7, n. 7, p. 19-40, 2018. DOI: https://doi.org/10.19135/revista.consinter.0007.01

OCDE. **A Caminho da Era Digital no Brasil.** Paris: OECD Publishing, 2020.

OLIVEIRA, Adriana Carla Silva de; ARAÚJO, Douglas da Silva. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, v. 16, n. 2, p. e5318, 2020. DOI: https://doi.org/10.18617/liinc.v16i2.5318

PAGANI, Regina Negri; KOVALESKI, João Luiz; RESENDE, Luis Mauricio. Methodi Ordinatio: a proposed methodology to select and rank relevant scientific papers encompassing the impact factor, number of citations, and year of publication. **Scientometrics**, v. 105, n. 40, p. 2109-2135, 2015. DOI: https://doi.org/10.1007/s11192-015-1744-x

PALHARES, Gabriela Capobianco; SANTOS, Alessandro Santiago dos; ARIENTE, Eduardo Altomare; GOMES, Jefferson de Oliveira. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. **Estudos Avançados**, v. 34, n. 99, p. 175-190, 2020. DOI: https://doi.org/10.1590/s0103-4014.2020.3499.011

PERRI, Six; RAAB, Charles; BELLAMY, Christine. Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy. Part I. **Public administration**, v. 83, n. 1, p. 111-133, 2005. DOI: https://doi.org/10.1111/j.0033-3298.2005.00440.x

PHILLIPS, Benjamin. UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. **Computer law and security report**, v. 42, n. 105586, 2021. DOI: https://doi.org/10.1016/j.clsr.2021.105586

PLEGER, Lyn E.; GUIRGUIS, Katharina; MERTES, Alexander. Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. **Computers in human behavior**, v. 122, n. 106830, p. 1-17, 2021. DOI: https://doi.org/10.1016/j.chb.2021.106830

ROCHA, Núbia Augusto de Sousa; ALMEIDA, Alexandre Nascimento de; BRAGA, Tiago Emmanuel Nunes; NUNES, André. O tratamento de dados pessoais pelo poder público: um estudo bibliométrico. **Liinc em Revista**, v. 19, n. 2, p. e6455, 2023. DOI: https://doi.org/10.18617/liinc.v19i2.6455.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

SARABDEEN, Jawahitha; CHIKHAOUI, Emma; ISHAK, Mohamed Mazahir Mohamed. Creating standards for Canadian health data protection during health emergency: An analysis of privacy regulations and laws. **Heliyon**, v. 8, n. 5, p. e09458, 2022. DOI: https://doi.org/10.1016/j.heliyon.2022.e09458

SGD – Secretaria de Governo Digital. **Lei Geral de Proteção de Dados (LGPD): Guia de Boas Práticas para Implementação na Administração Pública Federal.** Brasília, DF: SGD, 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf>. Acesso em 15 jul. 2023.

SOARES, Sandro Vieira; PICOLLI, Icaro Roberto Azevedo; CASAGRANDE, Jacir Leonir. Pesquisa bibliográfica, pesquisa bibliométrica, artigo de revisão e ensaio teórico em administração e contabilidade. **Administração: ensino e pesquisa**, v. 19, n. 2, p. 308-339, 2018. DOI: https://doi.org/10.13058/raep.2018.v19n2.970

STELZER, Joana. *et al*. A lei geral de proteção de dados pessoais e os desafios das instituições de ensino superior para a adequação. *In*: XIX Colóquio Internacional de Gestão Universitária, Florianópolis, 2019. **Anais** [...]. Florianópolis: CIGU, 2019. Disponível em: <https://repositorio.ufsc.br/handle/123456789/201939>. Acesso em: 14 jul. 2023.

SULE, Mary-Jane; ZENNARO, Marco; THOMAS, Godwin. Cybersecurity through the lens of digital identity and data protection: Issues and trends. **Technology in society**, v. 67, n. 101734, 2021. DOI: https://doi.org/10.1016/j.techsoc.2021.101734

TAYLOR, John A.; LIPS, Miriam; ORGAN, Joe. Identification practices in government: citizen surveillance and the quest for public service improvement. **Identity in the information society**, v. 1, n. 1, p. 135-154, 2008. DOI: https://doi.org/10.1007/s12394-009-0007-5

TEIXEIRA, Tarcísio; ARMELIN, Ruth, Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. São Paulo: Editora Saraiva, 2022.

TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão nº 1384/2022**, TCU/Plenário, 21 jun. 2022. Disponível em: <https://bit.ly/3MyEYFv>. Acesso em: 14 jul. 2023.

VAN SLYKE, Craig; SHIN, J. T.; JOHNSON, Richard; JIANG, James J. Concern for information privacy and online consumer purchasing. **Journal of the Association for Information Systems**, v. 7, n. 6, p. 415-444, 2006. https://doi.org/10.17705/1jais.00092

VAINZOF, Rony. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. (Coord.). **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2019.

Revista | Direitos Sociais e Políticas Públicas Unifafibe

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público. *In*: BIONI, Bruno Ricardo. (Org.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021.