ARTIGOS

O direito humano à privacidade e a governança de dados: oportunidades a partir do guia de políticas de governança de dados da NSCS

Felipe Fonseca Salerno
Antônio Carlos Gastaud Maçada

Resumo: Com o avanço das tecnologias digitais no Poder Judiciário Brasileiro, os tribunais armazenam um volume crescente de dados, ensejando esforços para a preservação do direito à privacidade no uso e divulgação dos dados. Esta pesquisa exploratória analisa oportunidades que a governança de dados apresenta em relação à privacidade. Para tanto, analisa-se o Guia de Políticas de Governança de Dados da NCSC, utilizado pelos tribunais norte americanos, e sua aderência às pesquisas sobre o tema. Ao final, são apresentadas nove oportunidades, que são recomendações aos tribunais para implementar e aprimorar a governança de dados, com intuito de assegurar o tratamento apropriado dos dados sensíveis e a preservação do direto à privacidade.

Palavras-chave: Governança de dados. Privacidade. Dados sensíveis. Poder Judiciário.

Abstract: With the advancement of digital technologies in the Brazilian Judiciary, the courts are storing an ever-increasing volume of data, giving rise to efforts to preserve the right to privacy in the use and disclosure of data. This exploratory research examines the opportunities *Data Governance* offers in relation to privacy. To this end, the NCSC *Data Governance* Policy Guide, used by the North American courts, is analyzed regarding its adherence to research in this matter. Consequently, nine recommendations are made to help courts implement and improve *Data Governance*, ensuring the appropriate treatment of sensitive data and preserving the right to privacy.

Keywords: *Data Governance*. Privacy. Sensitive data. Judiciary.

1 Introdução

A Declaração Universal dos Direitos Humanos, documento atualmente assinado por 193 países, traz em seu Artigo 12 o direito à privacidade, definido como

> Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (ONU, 2021).

Com o notório avanço das tecnologias digitais, o direito humano à privacidade está sob constante discussão nas Organizações Internacionais. Em relatório recente, o Alto Comissariado das Nações Unidas para os Direitos Humanos destacou a crescente preocupação com as vulnerabilidades em privacidade ocasionadas pelo avanço das tecnologias digitais. A publicação destaca que, apesar dos inegáveis avanços sociais proporcionados pelas novas tecnologias, há também uma crescente preocupação com o uso intensivo de dados pessoais e violação da privacidade (HRC, 2018).

Entre diversos programas para a promoção e preservação dos Direitos Humanos, existe a Agenda 2030, iniciativa da Organização das Nações Unidas (ONU), que consiste em um plano de ação com 17 Objetivos do Desenvolvimento Sustentável (ODS) e 149 metas, buscando garantir à população o acesso a direitos básicos, tais como a disponibilidade de água potável e o trabalho digno (AGENDA 2030, 2021).

Aderindo a essa iniciativa, o Conselho Nacional de Justiça (CNJ) foi a instituição responsável por formalizar a adesão do Poder Judiciário Brasileiro à Agenda 2030, sendo esse um movimento pioneiro no mundo. A partir do acordo firmado com a ONU, o CNJ passou a adotar rotineiramente ações visando o cumprimento dos ODS, nas quais destacase a criação do Laboratório de Inovação, Inteligência e ODS (LIODS) para monitoramento e promoção de ações voltadas ao alcance desses objetivos (CNJ, 2021a, 2021b).

Sob a perspectiva da gestão judiciária, destaca-se o ODS 16 — Paz, Justiça e Instituições Eficazes, cujo objetivo é "promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas em todos os níveis" (AGENDA 2030, 2021). Foram estabelecidas doze metas para o alcance desse objetivo, das quais destacam-se:

> 16.6 Desenvolver instituições eficazes, responsáveis e transparentes em todos os níveis
>
> 16.7 Garantir a tomada de decisão responsiva, inclusiva, participativa e representativa em todos os níveis

> 16.8 Ampliar e fortalecer a participação dos países em desenvolvimento nas instituições de governança global [...]
>
> 16.10 Assegurar o acesso público à informação e proteger as liberdades fundamentais, em conformidade com a legislação nacional e os acordos internacionais (AGENDA 2030, 2021).

Observa-se nas metas definidas pela ONU o conceito de governança, o qual é sintetizado por Gonçalves (2005) como a adoção de procedimentos e práticas para o alcance de objetivos, incluindo também a avaliação institucional do processo decisório. Todavia, o autor argumenta que a palavra governança por si só possui diversos significados, sugerindo analisá-la a partir de um foco específico.

Nesse sentido, o CNJ, em parceria com o Tribunal de Contas de União (TCU), disponibiliza o "Referencial Básico de Governança aplicável a Órgãos e Entidades da Administração Pública", publicação que tem como objetivo orientar sobre as melhores práticas em governança. Destaca-se dessa publicação o objetivo de "prover aos cidadãos dados e informações de qualidade (confiáveis, tempestivas, relevantes e compreensíveis)" (TCU, 2014, p. 14). Assim, analisa-se neste artigo a governança de dados, ou seja, focando o conceito de governança aos procedimentos, práticas e decisões que envolvem os dados da organização, com foco nas intersecções com o direito à privacidade.

A governança de dados (*Data Governance*, em inglês) é definida como uma estrutura multifuncional que auxilia a organização a gerenciar os dados como ativos estratégicos para o alcance de seus objetivos (ABRAHAM; SCHNEIDER; VOM BROCKE, 2019). Ladley (2019) aponta as vantagens de adotar políticas voltadas aos dados, como o aumento da qualidade da informação, a utilização de dados para a tomada de decisão e a consequente melhora na *performance* da organização.

Nesse contexto, a discussão sobre governança de dados é relevante considerando que o Poder Judiciário Brasileiro, sob a liderança do CNJ, estabelece esforços para incentivar o uso de tecnologias digitais, tais como o processo eletrônico (CNJ, 2021c). Para ilustrar esse avanço, o relatório "Justiça em Números 2020" demonstra que, em 2009, o percentual de processos eletrônicos era de 11,2%. Com incentivos a sua implantação, em 2019 esse percentual aumentou para 90%, indicando que o uso de tecnologias digitais é atualmente uma realidade para a maioria dos tribunais (CNJ, 2020).

Existem, todavia, pontos de atenção que acompanham a adoção de tecnologias digitais. A quantidade exponencial de dados que passam a ser armazenados pelos tribunais oferece a oportunidade de aprimorar o processo de tomada de decisão. No entanto, por outro lado, também gera riscos em relação ao uso inapropriado dos dados, ameaçando a segurança da informação e a preservação do direto à privacidade daqueles que procuram o Poder Judiciário.

Dessa forma, vislumbra-se que assegurar a governança de dados no Poder Judiciário é um desafio para a maturidade administrativa dos tribunais, uma vez que os dados tornar-se-ão fundamentais para incrementar a qualidade da gestão administrativa e judicial. Conforme Thompson, Ravindran e Nicosia (2015), em instituições públicas, existem desafios característicos em relação aos dados, tais como a frequente operacionalização de um grande volume de dados pessoais, o que exige cautela na utilização, tratamento, armazenagem e compartilhamento dos dados. Segundo os autores, a operacionalização desse grande volume de dados apresenta diversos riscos à privacidade das informações.

Internacionalmente, o debate sobre o direito à privacidade e a governança de dados também é uma realidade. O *National Center for State Courts* (Centro Nacional para Cortes Estaduais – NCSC), associação que promove políticas e debates sobre dados nos tribunais dos Estados Unidos, publicou recentemente o "Guia para Políticas de Governança de Dados", documento inovador que disserta sobre governança de dados no Poder Judiciário. Na publicação, é reforçada a utilização dos dados como ativos estratégicos para os tribunais, tanto para assegurar a qualidade administrativa quanto a jurisdicional. Também há seção dedicada ao tratamento de dados sensíveis, a qual debate o papel da governança e da proteção à privacidade (NCSC, 2019). Assim, o NCSC propõe um novo paradigma na utilização dos dados pelos tribunais, e conjectura-se que, por meio da análise desse guia, podem ser extraídas oportunidades de aprimorar a governança de dados nas cortes brasileiras.

Frente a relevância da discussão sobre o direito humano à privacidade e suas interações com a governança de dados, este artigo objetiva analisar oportunidades extraídas do "Guia de Governança de Dados da

NCSC" e sua aderência às pesquisas sobre o tema, buscando fornecer subsídios para a elaboração e aprimoramento da governança de dados no Poder Judiciário brasileiro.

Justifica-se este artigo por sua relevância estratégica para o Poder Judiciário brasileiro. Com mais de 70 milhões de processos pendentes (CNJ, 2020), os tribunais armazenam grande volume de dados sobre cidadãos e empresas, de maneira que assegurar o direito à privacidade é fundamental para garantir a segurança jurídica e o tratamento adequado das informações sob responsabilidade dos tribunais. Assim, vislumbra-se que contextualizar oportunidades da governança de dados propostas pelo NCSC (2019) sob a perspectiva da privacidade e dos tribunais brasileiros oferece a essas instituições a possibilidade de ganhos de eficiência operacional e consequente retorno à população na qualidade dos serviços.

Para tanto, a metodologia adotada foi a revisão da literatura sobre governança de dados, em um estudo exploratório, fazendo um paralelo entre o guia do NCSC (2019) e os principais autores sobre o tema (ABRAHAM; SCHNEIDER; VOM BROCKE, 2019; LADLEY, 2019; PLOTKIN, 2013). O desenvolvimento dar-se-á a partir da análise de tópicos fundamentais no contexto dos dados, que seriam: governança de dados e seus princípios, transparência, custos, responsabilização e tomada de decisão, qualidade do dado e ciclo de vida, e dados sensíveis. Para cada tópico são apresentadas as oportunidades em governança de dados e privacidade que podem ser exploradas pelo Poder Judiciário brasileiro a partir das medidas adotadas pelos tribunais norteamericanos. Ao final, é apresentada uma síntese dessas oportunidades, colaborando para a agenda de debates sobre o tema.

2 Desenvolvimento

Neste capítulo são expostas as discussões e análises relacionadas ao tema proposto. Para tanto, o conteúdo foi dividido em seções que abordam os principais tópicos desta pesquisa: governança de dados, princípios do NCSC da governança de dados, transparência, tipos de dados, custos, responsabilização e tomada de decisão, qualidade do dado e ciclo de vida, dados sensíveis. Ao final, são apresentadas as oportunidades identificadas, sintetizando o raciocínio desenvolvido em cada seção.

2.1 Governança de dados

A governança pode ser entendida como um meio que assegura as condições para o alcance de objetivos predeterminados (VENTURA; COELI, 2018). Ladley (2019) complementa esse conceito apontando que ele é relacionado ao exercício da autoridade para fins de configuração, administração, monitoramento e controle perante uma organização ou processo. Nesse sentido, considerando os procedimentos relacionados aos dados armazenados e utilizados pelas empresas, existe a governança de dados.

Lajara (2013) analisou a definição de governança de dados entre diferentes autores e publicações, destacando que o termo apareceu inicialmente em um artigo científico de 2004, e que desde então passou a ser recorrente nas publicações acadêmicas. Com o aumento das pesquisas e do volume de dados armazenados pelas empresas, estudos atuais exploram como a governança de dados colabora com a preservação do direito à privacidade dos usuários (CRAIG; LUDLOFF, 2011; SALIDO; VON, 2010).

Detalhando a definição, verifica-se que a governança de dados permite que as partes interessadas compreendam, priorizem e gerenciem os riscos relacionados com transmissão, acesso, uso, armazenamento e descarte dos dados (BOYD; RANDALL; FERRANTE, 2015). Plotkin (2013, p. 02, tradução nossa) sintetiza essa elucidação ressaltando que a governança de dados "tem mais a ver com o estabelecimento de funções e responsabilidades sobre como as pessoas gerenciam e tomam decisões sobre os dados do que sobre os dados em si". Em visão análoga, Ladley (2019) destaca que, independentemente da definição adotada, a governança de dados envolve o uso da autoridade em combinação com políticas visando assegurar que os ativos de informação tenham uma gestão adequada. Complementarmente, argumenta-se que para a implementação da governança de dados é necessário considerar, entre outros tópicos, o aspecto legal, o interesse público e a privacidade (BOYD; RANDALL; FERRANTE, 2015).

Logo, verifica-se, a partir das definições, que a governança de dados é um instrumento que permite às organizações gerarem valor a partir dos dados. No contexto do Poder Judiciário, em especial decorrente da adoção de tecnologias digitais, observa-se que ela desponta como uma oportunidade a ser explorada. Internacionalmente, verificase que há um crescente movimento

nesse sentido, destacando-se o "Guia de Políticas de Governança de Dados" publicado pelo NCSC. A publicação explora como os tribunais de justiça podem implementar políticas de governança de dados e as vantagens de adotá-las, incluindo questões de privacidade, cujo exame detalhado permite extrapolar oportunidades para o Poder Judiciário brasileiro.

Inicialmente, o NCSC destaca a contextualização da governança de dados no Poder Judiciário, argumentando que ela é essencial para sustentar o crescente volume de dados coletados e analisados pelas cortes (NCSC, 2019). De maneira similar ao sugerido pelos autores (LADLEY, 2019; PLOTKIN, 2013), a governança de dados é apresentada como um desdobramento da governança institucional, denominada governança dos tribunais pelo NCSC. Há convergência também na classificação de dados como ativos estratégicos, demonstrando que nos tribunais essa também é uma realidade.

> Os dados são ativos estratégicos para os tribunais, cada vez mais necessários não só para o funcionamento do tribunal e a gestão dos processos, mas também para o planejamento estratégico, o desenvolvimento de políticas e orçamentos e a melhoria do desempenho dos tribunais. Esta é uma mudança significativa da visão dos dados existentes principalmente como subprodutos do processamento de casos ou gestão do tribunal (NCSC, 2019, p. 2, tradução nossa).

O NCSC (2019) também destaca a eficiência promovida pela governança de dados, argumentando que ela "aumenta a eficiência e melhora a comunicação alinhando as práticas de dados em diferentes tribunais dentro do mesmo estado ou território" (NCSC, 2019, p. 2, tradução nossa). Ladley (2019) também argumenta nesse sentido, apontando que a governança de dados auxilia na eficiência da organização por meio da integração entre diferentes unidades por meio do compartilhamento de dados.

No contexto do Poder Judiciário brasileiro, o alinhamento de termos e conceitos nos diferentes tribunais foi aperfeiçoado por meio da Resolução CNJ n. 76, de 12 de maio de 2009, a qual instituiu o Justiça em Números (BRASIL, 2009). Essa resolução apresentou um glossário com a definição e forma de cálculo de diversas variáveis de interesse do Poder Judiciário, assegurando que todos os tribunais divulgassem informações utilizando os mesmos parâmetros. Cita-se ainda o DataJud, plataforma de armazenamento centralizado de dados e metadados, em implementação pelo CNJ, que também viabiliza o alinhamento das práticas de coleta de dados entre os diferentes tribunais, colaborando para uma comunicação mais alinhada entre as instituições do Poder Judiciário (CNJ, 2021d).

Portanto, evidencia-se que a governança de dados fornece uma visão dos dados como ativos estratégicos para os tribunais, destacando-se seu potencial para a melhoria do desempenho e da gestão. Percebe-se, por conseguinte, uma oportunidade:

> I) Instituir políticas e procedimento de governança de dados que tratem os dados como ativos estratégicos dos tribunais.

Identificada uma oportunidade a partir do conceito geral de governança de dados, explora-se como o NCSC (2019) aborda outros conceitos propostos pela literatura, os quais serão apresentados nas seções seguintes.

2.2 Princípios NCSC da governança de dados

O NCSC (2019) destaca princípios básicos da governança de dados, adaptando sua interpretação à realidade dos tribunais. A exposição dos princípios norteia as políticas de governança, sendo um referencial a ser observado pelos gestores em todas as etapas da implementação. Conforme a publicação, os princípios são:

a) Considerar os dados do tribunal como um ativo estratégico, não simplesmente como um subproduto do gerenciamento de processos
b) Estabelecer e manter a qualidade dos dados como parte do plano estratégico e da prática diária dos tribunais.
c) Identificar o servidores-chave e responsáveis para governança e qualidade de dados.
d) Ter padrões de dados práticos em vigor. Padrões de dados são as regras pelas quais os dados são descritos. Devem ser consistentes com as políticas e práticas do tribunal e fazer sentido para os usuários do tribunal.
e) Ter um plano e uma estratégia consistente para identificar e resolver problemas de dados.
f) Inovar e aprender as partes principais da cultura do tribunal.

g) Saber que surgirão disputas sobre os dados e estabelecer um mecanismo para resolver conflitos entre as partes interessadas. (NCSC, 2019, p. 4, tradução nossa).

Observa-se que os princípios enumerados pelo NCSC (2019) são convergentes com a literatura em governança de dados (LADLEY, 2019; LAJARA, 2013; PLOTKIN, 2013), destacando-se a visão de dados como ativos estratégicos, a definição de políticas e padrões e a definição de responsáveis pelos dados, aspectos fundamentais na implementação da governança de dados. Soma-se ainda a necessidade de investir os recursos necessários, tanto de pessoal quanto de maquinário, para que a governança de dados seja efetiva no dia a dia dos tribunais.

Dada a importância dos princípios como norteadores aos gestores, conjectura-se uma oportunidade aos tribunais brasileiros:

> II) Estabelecer princípios para orientar gestores na implementação e execução das políticas de governança de dados.

A seção seguinte explora a transparência e suas intersecções com o tema.

2.3 Transparência

A publicação disserta também sobre como a transparência em instituições públicas aumentou a demanda por dados, expondo que a divulgação de informações precisas e confiáveis são esperadas pela população (NCSC, 2019). Conforme o Instituto Brasileiro de Governança Corporativa (IBGC), a transparência é um dos quatro princípios da governança corporativa, juntamente com equidade, prestação de contas e responsabilidade corporativa (IBGC, 2015). Logo, a governança de dados colabora para o alcance do princípio da transparência, uma vez que organiza e define critérios para a publicação dos dados disponibilizados à população.

No contexto da transparência e do direito à privacidade, observa-se que a governança de dados possui potencial de reduzir o risco de divulgação de que dados sensíveis ao público a partir da definição de políticas e critérios para a publicação de informações. Menciona-se a Lei n. 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais, contemplando, inclusive, a divulgação em meios digitais como o Portal Transparência (BRASIL, 2018a).

Ladley (2019) comenta que a governança de dados deve estar alinhada com a regulação legal, prezando pela conformidade e assim colaborando para a redução de riscos regulatórios. Dessa forma, há de se observar critérios legais para assegurar que informações pessoais sensíveis não são divulgadas ao público, sendo a governança de dados uma ferramenta para mitigar esse risco.

Focando esse debate no Poder Judiciário, o CNJ realiza anualmente o Ranking Transparência, instituído pela Resolução CNJ n. 260, de 11 de setembro de 2018, iniciativa que premia tribunais a partir da verificação da conformidade nas publicações do portal transparência. Enfatiza-se nessa premiação a pontuação ao tribunal por divulgação de dados abertos, estruturados e legíveis por máquinas (BRASIL, 2018b). Sugere-se que, para atender a esse requisito, os tribunais devem possuir mecanismos mínimos de governança de dados que possibilitem a geração, armazenamento e divulgação dos dados para atender ao requisito estabelecido pelo CNJ. Ainda, infere-se a necessidade de políticas para assegurar o direito à privacidade, garantindo que dados sensíveis não serão disponibilizados.

Logo, no contexto da transparência e do direito à privacidade, observa-se que a governança de dados, a partir da definição de políticas e critérios para a publicação de informações, reduz o risco de divulgação de dados sensíveis ao público. Assim, entende-se uma oportunidade ao Poder Judiciário brasileiro:

> III) Definir políticas e critérios para os dados destinados à publicação no Portal Transparência e à divulgação em geral.

Identificada a oportunidade a partir da relação entre transparência e privacidade, a próxima seção disserta sobre os tipos de dados contextualizados ao Poder Judiciário, conforme proposto por NCSC (2019).

2.4 Tipos de dados

Sobre os tipos de dados que são utilizados pelas cortes, o NCSC (2019) sugere sete classificações, que são expostas no Quadro 1. Conforme a publicação, em virtude dos tribunais armazenarem e fornecerem diversos dados, é interessante que a política de

governança de dados aborde a maior variedade possível de classificações, sob o risco de redundância e retrabalho na coleta, armazenagem e uso dos dados. Verifica-se a partir da sugestão que há três principais fontes de dados: sistemas judiciais, sistemas administrativos e sistemas suplementares. Observa-se também que há modificação na classificação conforme o tratamento do dados: sem tratamento, compilado, agregado.

Quadro 1 – Classificação quanto ao tipo de dado

Classificação do dado	Descrição
Dados de gerenciamento de processos judiciais	São dados utilizados nos processos judiciais, normalmente armazenados nos sistemas judiciais. São elementos típicos a data de ingresso, de baixa, grau, partes, decisões, etc.
Dados em Massa	São dados extraídos dos sistemas judiciais sem modificação ou compilação.
Dados Compilados	São dados extraídos e compilados de um ou mais processos judiciais ou administrativos, trabalhados para um objetivo específico.
Dados Administrativos	São os dados utilizados na gestão administrativa dos tribunais, tais como informações sobre magistrados e servidores, exames, educação, etc.
Dados Agregados	São relatórios, pareceres, normalmente apresentados de forma anual. São utilizados para medir a performance dos tribunais. Podem utilizar dos demais tipos de dados para sua construção
Dados Suplementares	São dados que não estão incluídos nos sistemas judiciais ou administrativos mas que auxiliam para atividades diversas, como cadastro de intérpretes, agendamentos, contabilidade, etc.
Produto de Trabalho	São e-mails, dados, apresentações, relatórios e outros elementos usados internamente que auxiliam na tomada de decisão.

Fonte: NCSC (2019, tradução nossa).

Em paralelo com a literatura, analisa-se que a classificação adotada pelo NCSC (2019) é bem específica ao contexto dos tribunais. Ladley (2019) e Plotkin (2013) argumentam que conhecer os dados da organização é fundamental para estabelecer políticas de governança de dados. Complementa-se argumentando que a identificação dos tipos de dados é fundamental para a posterior responsabilização e definição dos direitos de decisão, os quais são fundamentais para a implementação da governança de dados.

Sob o prisma da privacidade, a classificação dos dados permite identificar a presença de dados sensíveis, colaborando para a definição de políticas para sua preservação. Argumenta-se que sem a referida classificação não é possível saber quais dados devem ser preservados, sendo essa identificação um passo inicial no processo de garantia da privacidade (TORRA; NAVARRO-ARRIBAS, 2014).

Logo, observa-se que a classificação proposta pelo NCSC (2019) pode auxiliar tribunais brasileiros a identificarem os tipos de dados em seu domínio, colaborando para a implementação de políticas de governança de dados. Dessa forma, observa-se uma oportunidade:

> IV) Identificar e catalogar os tipos de dados armazenados e utilizados pelos tribunais de maneira a subsidiar as políticas de governança de dados.

A seção seguinte explora os custos apontados pelo NCSC (2019) como associados com a ausência de políticas de governança de dados.

2.5 Custos

Esta seção apresenta a visão do NCSC (2019) em relação aos custos que os tribunais se submetem ao não adotarem políticas de governança de dados. Alega-se que, para cada custo, há um ganho ser explorado pelas cortes. São apresentados os seguintes prejuízos:

> Tempo gasto procurando informações perdidas;
>
> Entrada redundante de dados;
>
> Diminuição da produtividade;
>
> Limpeza de dados;
>
> Dificuldade em tomar decisões devido a dados incompletos ou imprecisos;
>
> Incapacidade de conduzir avaliações significativas;
>
> Moral do pessoal;
>
> Tempo gasto tomando decisões repetitivas porque a política não é clara.
>
> (NCSC, 2019, p. 4-5, tradução nossa).

Novamente, verifica-se que a abordagem utilizada pelo NCSC (2019) é convergente com a literatura sobre governança de dados. Lajara (2013) apresenta uma revisão sobre o conceito de governança de dados, demonstrado a partir de diferentes autores sua relação com custos, que pode se apresentar de maneira direta — como o custo de produzir e armazenar dados — e indireta — referente ao impacto da baixa qualidade dos dados no desempenho organizacional. Abraham, Schneider e Vom Brocke (2019) também apontam que a governança de dados colabora para minimizar custos e riscos relacionados a dados, sugerindo que sua ausência faz com que as organizações gastem tempo em atividades que não agregam valor aos dados.

Sob o contexto da privacidade, os autores (ACQUISTI; FRIEDMAN; TELANG, 2006; SORIA-COMAS; DOMINGO-FERRER, 2016) comentam sobre o impacto da preservação da privacidade nos custos organizacionais, debatendo sobre o trade-off entre o investimento em políticas de segurança e um eventual vazamento de informações. Para o Poder Judiciário, verifica-se que a proteção da privacidade é parte intrínseca de suas atividades, sendo sua preservação fundamental para a garantia da tutela jurisdicional (ÁVILA; WOLOSZYN, 2017).

Dessa forma, identifica-se uma oportunidade a ser explorada pelos tribunais brasileiros no que se refere à identificação de custos, sendo este o primeiro passo para subsidiar o desenvolvimento de políticas de governança de dados:

> V) Identificar os custos relacionados aos dados.

A próxima seção explora um conceito-chave em governança: a definição de papéis e responsabilidades na estrutura organizacional.

2.6 Responsabilização e tomada de decisão

Acerca da responsabilização e tomada de decisão, a publicação aponta que é fundamental decidir os responsáveis pelos dados, que "qualquer política de governança de dados precisa abordar quem é o proprietário dos dados e quem pode liberá-los" (NCSC, 2019, p. 11, tradução nossa). Essa visão é semelhante com a de Plotkin (2013), que utiliza o conceito de *data ownership* (propriedade dos dados, em tradução literal) e de *data stewards* (mordomo dos dados, em tradução literal), posições dentro da organização que representam autoridades perante os dados, sendo responsáveis pela tomada de decisão e manutenção da qualidade das informações entre os diferentes níveis organizacionais.

Destaca-se, além desses conceitos, a recomendação pelo NCSC (2019) da criação de um Conselho ou Comitê de Governança de Dados, o qual seria responsável por decisões relacionadas à estratégia. Sobre sua estrutura, sugere que seja composta por um grupo multidisciplinar, que compreenda tanto do negócio como da tecnologia envolvida nos sistemas. Argumenta-se que, em virtude da governança de dados ser dinâmica, o Comitê deve avaliar e refinar as políticas, tanto de maneira periódica como extraordinária para resolução de problemas.

Além do Comitê, é sugerida a definição de um diretor de informação (*chief information office* – CIO) e um diretor dos dados (*chief data officer* – CDO). Apesar de ambos os cargos estarem relacionados com a governança de dados, existem diferenças nas suas atribuições e responsabilidades, que são apresentadas na Quadro 2. Em contraponto a essa estrutura, Ladley (2019) recomenda que a governança de dados não esteja sob responsabilidade do CIO, uma vez que ela deve estar alinhada com os processos de negócio, sugerindo que a abordagem tecnológica do CIO pode ser um obstáculo para a implementação do programa de governança. Assim, propõe-se que o tema fique sob responsabilidade do CDO, que possui conhecimento do negócio para viabilizar o alinhamento entre os dados e a geração de valor para a organização.

Outras posições apresentadas pelo NCSC (2019) são os gestores de dados públicos, responsável por avaliar dados remetidos para divulgação externa; os analistas de qualidade de dados, pessoas qualificadas para identificar e avaliar conformidades e desconformidades em qualidade; e os *data stewards*, especialistas que auxiliam nas ações referentes aos dados de sua *expertise*. Cita-se que, para o exercício dessas funções, não é necessário dedicação exclusiva, podendo as responsabilidades serem exercidas concomitantemente com outra função. O Quadro 3 apresenta as responsabilidades de cada função para governança de dados.

Quadro 2 –Principais funções e responsabilidades para a governança de dados

Comitê de Governança de Dados	**Diretor de Informação (Chief Information Office – CIO)**	**Diretor dos Dados (Chief Data Officer – CDO)**
Composição: • Pesquisadores e estatísticos; • Profissionais de tecnologia da informação (TI); • Servidores responsáveis pela entrada direta de dados; • Magistrados e servidores que usam / revisam / consomem dados; • Representantes regionais; • Gabinete de relações públicas ou informação pública; • Consultor jurídico geral; • Articulação legislativa. Responsabilidades: Avaliar e refinar, ordinariamente e extraordinariamente, as políticas de governança de dados.	Responsabilidades: Fornecer a capacidade de capturar, medir e rastrear dados; Selecionar e implementar tecnologia para cumprir requisitos do negócio; Focar na governança tecnológica; Supervisionar servidores responsáveis por hardware e software.	Responsabilidades: Fornecer a capacidade de encontrar sentido nos dados; Definir requisitos de dados para cumprir requisitos do negócio; Focar na governança de dados; Supervisionar ou trabalhar em conjunto com os data stewards e analistas de dados.

Fonte: NCSC (2019, tradução nossa).

Quadro 3 – Funções auxiliares e responsabilidades para a governança de dados

Gestor de Dados Públicos	Analista de Qualidade dos Dados	Data Stewards
Responsabilidades: Receber e avaliar solicitações de dados destinados ao público; Garantir que os dados em um site público sejam atualizados, completos e apropriados.	Responsabilidades: Atuar como analista de processos de negócios, verificando se os processos estabelecidos são seguidos com fidelidade; Executar e monitorar relatórios de qualidade de dados; Responder a relatórios de problemas de qualidade de dados; Educar outras equipes sobre a importância da qualidade de dados; Reconhecer a excelência em qualidade de dados; Realizar treinamento sobre processos de negócios e qualidade de dados.	Responsabilidades: Fazer recomendações ao Comitê de Governança de Dados sobre questões relativas aos dados de sua expertise; Aprovar a divulgação de dados agregados relacionados a sua expertise; Participar nas decisões sobre a troca de dados relacionados a sua expertise; Monitorar a qualidade dos dados relacionados a sua expertise; Validar a precisão dos dados relacionados a sua expertise; Verificar se os dados de sua expertise são adequados para divulgação.

Fonte: NCSC (2019, tradução nossa).

Acerca da privacidade, verifica-se que a definição de papéis e responsabilidades permite um maior controle acerca dos dados sensíveis, viabilizando a identificação de possíveis lacunas no controle e tratamento dos dados. Bennett e Raab (2020) argumentam que a governança possui uma relação direta com a privacidade, em que políticas internas da organização devem refletir os requisitos legais de proteção aos dados. Nesse sentido, definir responsáveis pela preservação dos dados é requisito básico para que a organização atue em conformidade com o ambiente legal, viabilizando a operacionalização dessas políticas no desenvolvimento das atividades do negócio.

Dessa forma, verifica-se dentro do conceito de governança de dados a necessidade de definir posições dentro da organização que sejam responsáveis pelos dados, assegurando que os requisitos de privacidade sejam atendidos. A criação e o exercício de funções específicas, com atribuições mapeadas, mostram-se fundamentais para que a governança de dados atinja seus objetivos, agregando valor à organização. Assim, evidencia-se uma oportunidade ao Poder Judiciário brasileiro:

> VI) Definir autoridades e responsáveis pelos dados dentro da estrutura organizacional.

A seção seguinte explora o conceito de qualidade do dado, expondo as considerações apresentadas pela literatura.

2.7 Qualidade do dado e ciclo de vida

O NCSC (2019) disserta também sobre o ciclo de vida dos dados, reforçando que a política de governança de dados deve considerar desde a coleta até o descarte. Visão semelhante é apresentada por Plotkin, que utiliza o conceito de cadeia da informação (*information chain*), argumentando que "processos de ciclo de vida de informações cuidadosamente planejados, documentados e executados protegem a qualidade dos dados" (2013, p. 43, tradução nossa). A Figura 1 demonstra o modelo proposto pelo NCSC, em que se verifica cinco principais etapas dentro desse ciclo. Comenta-se que a governança de dados desempenha um papel fundamental, instruindo e responsabilizando usuários sobre os procedimentos adequados em cada etapa do ciclo de vida.

Figura 1 – Ciclo de Vida dos dados

Fonte: NCSC (2019, p. 10, tradução nossa).

Sobre dificuldades em garantir a qualidade dos dados, são apresentados desafios comuns para as organizações: inconsistência de termos, informações inseridas incorretamente no sistema, migração de dados entre diferentes sistemas, expectativas do usuário desalinhadas, importação de dados externos, entre outros (RICKARDS; RITSERT, 2012). Os autores também apontam que um dado de melhor qualidade colabora para a redução de custos, além de criar valor para empresa por meio de relatórios confiáveis e precisos. Modi, Rao e Patel (2010) reforçam a importância de utilizar técnicas que permitam trabalhar com dados de qualidade e concomitantemente preservar a privacidade dos usuários. Talha, Kalam e Elmarzouqi

(2019) discutem que é preciso avaliar o *trade off* entre qualidade e segurança dos dados, sendo desejável um balanceamento entre essas características para viabilizá-los simultaneamente.

Considerando que um dos benefícios da governança de dados é melhorar a qualidade dos dados (LADLEY, 2019), verifica-se que a implementação de políticas pode colaborar para o alcance do padrão desejado. Nesse sentido, compreender cada etapa do ciclo de vida da informação é fundamental para a definição de ações adequadas a cada estágio. Dessa forma, assegura-se também que as iniciativas adotadas orientem em relação aos dados que oferecem riscos à privacidade, independentemente da etapa do ciclo que se encontre. Verifica-se, portanto, uma oportunidade:

> VII) Criar indicadores de *performance* para avaliar a qualidade dos dados a partir de seu ciclo de vida, em especial para a privacidade.

A próxima seção explora como o NCSC aborda os dados sensíveis.

2.8 Dados sensíveis

Em relação explícita com o direito à privacidade, o NCSC dedica-se a ressaltar a importância do tratamento adequado dos dados sensíveis em posse dos tribunais. São citados diversos pontos de atenção para o tratamento e armazenagem de dados, tais como informações sobre a saúde, tanto física quanto mental; informações financeiras; dados de nacionalidade, raça e endereço. Para os processos criminais, o NCSC sugere reforçar políticas de controle para informações sensíveis, como, por exemplo, a proteção dos dados de testemunhas e de jurados (NCSC, 2019).

Ainda sobre a proteção à privacidade em tribunais, são definidas questões para identificar oportunidades de melhoria no que tange à governança de dados sensíveis. Conforme o NCSC, é importante definir:

> Qual a necessidade do dado?
>
> Quem precisa ter acesso ao dado?
>
> Como limitar o acesso a dados sensíveis apenas para quem tem legitimidade para acessá-los?
>
> Se o tribunal coleta dados potencialmente sensíveis, há leis ou normas que regulam pedidos de informação? Sob quais circunstâncias?
>
> Quem será atingido caso ocorra um vazamento de dados?
>
> Quais as medidas existentes para proteger os dados sensíveis em caso de vazamento?
>
> O que é armazenado nos campos de dados e o que está disponível apenas em um documento?
>
> Se os documentos tiverem que ser preenchidos, esta é uma responsabilidade da parte que registra o processo ou do escrivão?
>
> Se um campo ou documento for configurado para ser lacrado ou confidencial, qual é o processo para substituir o padrão? (NCSC, 2019, p. 11, tradução nossa).

Complementando o exposto na Seção 2.6, é apontada a importância da definição de uma estrutura de tomada de decisão em relação aos dados, em abordagem similar a Ladley (2019) e Plotkin (2013). Especificamente sobre dados sensíveis, o NCSC recomenda que o Comitê de Governança de Dados delibere sobre quais dados são considerados confidenciais, enquanto o departamento de tecnologia da informação decida qual a melhor maneira de proteger dados confidenciais (NCSC, 2019),

Logo, observa-se oportunidades que podem ser replicadas pelo Poder Judiciário Brasileiro no que se refere à governança de dados e à proteção à privacidade a partir do guia norte-americano. São elas:

> VIII) Elaborar de uma política centralizada para a governança de dados nos tribunais, detalhando como serão operacionalizadas ações que envolvam dados sensíveis e proteção da privacidade;
>
> IX) Definir os papéis de tomada de decisão, acompanhamento, controle e monitoramento da política de governança de dados dentro do tribunal.

A próxima seção apresenta a síntese das oportunidades que foram identificadas ao longo do desenvolvimento.

2.9 Oportunidades

Após a revisão do Guia de Políticas de Governança de Dados do NCSC, que apresenta as diretrizes para a governança de dados nos tribunais norte-americanos, e seu paralelo com autores referência no tema, foram identificadas nove oportunidades aos tribunais brasileiros. Essas oportunidades representam recomendações às cortes brasileiras para implementar e aprimorar a governança de dados, com intuito de assegurar o tratamento apropriado aos dados

sensíveis e a preservação do direto à privacidade. O Quadro 4 apresenta a síntese desses achados.

Quadro 4 – Síntese das oportunidades de implementação e aprimoramento da governança de dados

Oportunidades identificadas no Guia de Políticas de Governança de Dados das cortes norte-americanas (NCSC, 2019)	Vantagens em relação à privacidade
Instituir políticas e procedimento de governança de dados que tratem os dados como ativos estratégicos dos tribunais;	Tratamento da privacidade em relação aos dados como ativo estratégico dos tribunais, empregando esforços para sua proteção em todos os níveis organizacionais.
Estabelecer princípios para orientar gestores na implementação e execução das políticas de governança de dados;	Assegurar que as pessoas na organização tenham conhecimentos dos princípios e políticas que versem sobre a preservação da privacidade no armazenamento, uso e divulgação dos dados;
Definir políticas e critérios para os dados destinados à publicação no Portal Transparência e a divulgação em geral;	Garantir que os dados disponibilizados ao público respeitem o direito à privacidade, observando o alinhamento entre políticas internas e leis nacionais de proteção de dados;
Identificar e catalogar os tipos de dados armazenados e utilizados pelos tribunais de maneira a subsidiar as políticas de governança de dados.	Identificar dados sensíveis cuja manejo inapropriado pode ocasionar violações de privacidade;
Identificar os custos relacionados aos dados;	Analisar o custo de proteger dados sensíveis e garantir a privacidade, com intuito de subsidiar a formulação de políticas de governança;
Definir autoridades e responsáveis pelos dados dentro da estrutura organizacional;	Garantir a responsabilização no uso de dados sensíveis, possibilitando que as decisões sobre dados que afetem à privacidade possuam alçada definida;
Criar indicadores de performance para avaliar a qualidade dos dados a partir de seu ciclo de vida, em especial para a privacidade;	Possibilitar o acompanhamento sistemático da qualidade dos dados, viabilizando a identificação de desconformidades em relação a dados sensíveis;
Elaborar uma política centralizada para a governança de dados nos tribunais, detalhando como serão operacionalizadas ações que envolvam dados sensíveis e proteção da privacidade;	Organizar a estrutura de tomada de decisão para dados relacionados à privacidade;
Definir os papéis de tomada de decisão, acompanhamento, controle e monitoramento da política de governança de dados dentro do tribunal.	Assegurar que as pessoas tenham conhecimento de suas responsabilidades em relação ao acompanhamento, controle e monitoramento de dados sensíveis.

Fonte: Elaborado pelos autores a partir de NCSC (2019).

Verifica-se a partir desta revisão que existem oportunidades a serem exploradas nos diferentes níveis organizacionais. Estrategicamente, a constituição de um Comitê de Governança de Dados permite que sejam definidas políticas de proteção à privacidade no armazenamento, uso e compartilhamento dos dados. O nível tático atua no sentido de assegurar que essas políticas possuam efetividade nos níveis inferiores, fazendo o elo entre a operacionalização e a conformidade com as atividades de governança. Por fim, operacionalmente deve-se difundir que a preservação da privacidade é um ativo para os tribunais, orientado procedimentos de inserção de dados nos sistemas e limitando o compartilhamento de informações sensíveis.

Apresentadas as oportunidades identificadas a partir do Guia de Políticas de Governança do *National Center for State Courts* norte-americano (NCSC, 2019), partese para a conclusão desta pesquisa, retomando os principais achados que poderão auxiliar os tribunais brasileiros na preservação da privacidade a partir da governança de dados.

3 Conclusão

Logo, o presente artigo analisou as oportunidades que a governança de dados oferece no que tange à garantia do direito à privacidade a partir do Guia de Políticas de Governança de Dados do *National Center for State Courts* (Centro Nacional para Cortes Estaduais – NCSC). Para tanto, foi realizada revisão da literatura sobre governança de dados, fazendo um paralelo com o apresentado pelo NCSC e com autores renomados nessa área de conhecimento. Foram identificadas nove oportunidades de aprimorar a governança de dados e de estimular a proteção de dados sensíveis pelos tribunais brasileiros, iniciativas cuja implementação reflete na preservação do direito à privacidade.

A contribuição deste artigo consiste na apresentação inédita de oportunidades em governança de dados a partir do NCSC, confirmando-se que as definições e iniciativas propostas pela organização são alinhadas com as pesquisas em governança de dados. As oportunidades identificadas no Quadro 4 auxiliam na definição de estratégias pelos tribunais, colaborando para a preservação da privacidade no uso e compartilhamento de dados e na responsabilização dos gestores. Contribui-se também ao elucidar as vantagens da implementação da governança de dados, a qual colabora com o aumento da eficiência e, consequentemente, com a qualidade dos serviços oferecidos aos cidadãos pelo Poder Judiciário brasileiro.

Acerca das limitações desta pesquisa, trata-se de um estudo exploratório, carecen-

do maior aprofundamento em relação ao tema. Para estudos futuros, sugere-se avaliar as similaridades e dissimilaridades do modelo proposto pelo NCSC com as políticas promovidas pelo CNJ, entre as quais o Datajud e o Justiça 4.0. Recomendase também avaliar em maior profundidade a privacidade sob a visão da LGPD e seus reflexos na administração dos dados em tribunais brasileiros.

Referências

ABRAHAM, R.; SCHNEIDER, J.; VOM BROCKE, J. *Data Governance*: A conceptual framework, structured review, and research agenda. **International Journal of Information Management**, v. 49, 2019. Disponível em: https://www.researchgate.net/publication/334653735_Data_Governance_A_conceptual_framework_structured_review_and_research_agenda#:~:text=Data%20governance%20refers%20to%20the,data%2Drelated%20cost%20and%20risk. Acesso em: 20 fev. 2021.

ACQUISTI, A; FRIEDMAN, A.; TELANG, R. Is There a Cost to Privacy Breaches? An Event Study. **ICIS 2006 Proceedings**, v. 94, 2006. Disponível em: http://aisel.aisnet.org/icis2006/94. Acesso em: 15 mar. 2021.

AGENDA 2030. **A Integração dos ODS**. 2021. Disponível em: http://www.agenda2030.com.br/os_ods/. Acesso em: 19 mar. 2021.

ÁVILA, A. P.; WOLOSZYN, A. L. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, v. 4, n. 3. p. 167-200, set./dez. 2017. Disponível em: https://revistas.ufpr.br/rinc/article/view/51295. Acesso em: 02 abr. 2021.

BENNETT, C.; RAAB, C. Revisiting the governance of privacy: Contemporary policy instruments in global perspective. **Regulation & Governance**, v. 14, p. 447–464, 2020. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12222. Acesso em: 20 mar. 2021.

BOYD, J.; RANDALL, S.; FERRANTE, A. Application of privacy-preserving techniques in operational record linkage centres. Medical **Data Privacy Handbook**, Springer, p. 267-287. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-23633-9_11. Acesso em: 05 mar. 2021.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 mar. 2021.

CNJ – CONSELHO NACIONAL DE JUSTIÇA. **Agenda 2030 no Poder Judiciário**. Brasília: CNJ, 2021b. Disponível em: https://www.cnj.jus.br/programas-e-acoes/agenda-2030/. Acesso em: 20 março 2021.

CNJ - CONSELHO NACIONAL DE JUSTIÇA. **DATAJUD**. Brasília: CNJ, 2021d. Disponível em: https://www.cnj.jus.br/sistemas/datajud/. Acesso em: 16 mar. 2021.

CNJ – CONSELHO NACIONAL DE JUSTIÇA. **LIODS CNJ** : Laboratório de Inovação, Inteligência e ODS. Brasília: CNJ, 2021a. Disponível em: https://www.cnj.jus.br/programas-e-acoes/agenda-2030/liods-cnj-laboratorio-de-inovacao-inteligenica-e-ods/. Acesso em: 25 mar. 2021.

CNJ – CONSELHO NACIONAL DE JUSTIÇA. **Justiça 4.0**. Brasília: CNJ, 2021c. Disponível em: https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/. Acesso em: 20 mar. 2021.

CNJ - CONSELHO NACIONAL DE JUSTIÇA. **Relatório Justiça em Números 2020**. Brasília: CNJ, 2020. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf. Acesso em: 25 mar. 2021.

CNJ – CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 76 de 12 de maio de 2009**. Dispõe sobre os princípios do Sistema de Estatística do Poder Judiciário, estabelece seus indicadores, fixa prazos, determina penalidades e dá outras providências. Brasília, DF: Conselho Nacional de Justiça, 2009. Disponível em: https://atos.cnj.jus.br/atos/detalhar/110. Acesso em: 20 mar. 2021.

CNJ – CONSELHO NACIONAL DE JUSTIÇA. **Resolução nº 260 de 11 de setembro de 2018**. Altera a Resolução CNJ n. 215, de 16 de dezembro de 2015, e institui o ranking da transparência do Poder Judiciário. Brasília, DF: Conselho Nacional de Justiça, 2018b. Disponível em: https://atos.cnj.jus.br/atos/detalhar/2694. Acesso em: 28 mar. 2021.

CRAIG, F.; LUDLOFF, M. **Privacy and Big Data**. Sebastopol: O'Reilly Media, 2011.

GONÇALVES, A. O conceito de governança. In: Congresso Nacional do CONPEDI/UEA, XV. **Anais de Congresso**. Manaus, 2006. Disponível em: https://egov.ufsc.br/portal/conteudo/o-conceito-de-governan%C3%A7a. Acesso em: 2 mar. 2021.

HRC - HUMAN RIGHTS COUNCIL. **The right to privacy in the digital age**: report of the united nations high commissioner for human rights. HRC, 2018. Disponível em: ht-

tps://undocs.org/A/HRC/39/29. Acesso em: 2 abr. 2021.

IBGC - INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**: CMPGC. São Paulo: IBGC, 2015. Disponível em: www.ibgc.org.br. Acesso em: 5 fev. 2021.

LADLEY, J. **Data Governance**: how to design, deploy, and sustain an effective *Data Governance* program. 2. Th. Londres: Academic Press, 2019.

LAJARA, T. **Governança da informação na perspectiva do valor, qualidade e compliance**: estudo de casos múltiplos. 2013, 156 f. Dissertação (Mestrado em Administração) – Escola de Administração, Universidade Federal do Rio Grande do Sul. Rio Grande do Sul, Porto Alegre, 2013.

MODI, C. N.; RAO, U. P.; PATEL, D. R. Maintaining privacy and data quality in privacy preserving association rule mining. **Second International Conference on Computing, Communication and Networking Technologies**, Karur, India, p. 1-6, 2010. Disponível em: https://ieeexplore.ieee.org/document/5592589. Acesso em: 15 mar. 2021.

NCSC - NATIONAL CENTER FOR STATE COURTS. **Data Governance Policy Guide**. Williamsburg: Court Statistics Project, 2019. Disponível em: https://www.courtstatistics.org/__data/assets/pdf_file/0014/23900/data-governance-final.pdf. Acesso em: 02 mar. 2021.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Universal Declaration of Human Rights**: Portuguese. ONU, 2021. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 02 abr. 2021.

PLOTKIN, D. **Data stewardship**: an actionable guide to effective data management and *Data Governance*. Waltham: Morgan Kaufmann, 2013.

RICKARDS, R.; RITSERT, R. *Data Governance*: Challenges Facing Controllers. **International Journal of Business, Accounting, and Finance**, v. 6, p. 25-42, 2012. Disponível em: https://www.researchgate.net/publication/339713098_Data_Governance_Challenges_Facing_Controllers. Acesso em: 21 mar. 2021.

SALIDO, J; VON, P. **A Guide to Data Governance for Privacy, Confidentiality, and Compliance**. Redmond: Microsoft, 2010. Disponível em: https://iapp.org/media/pdf/knowledge_center/Guide_to_Data_Governance_Part1_The_Case_for_Data_Governance_whitepaper.pdf. Acesso em: 15 fev. 2021.

SORIA-COMAS, J.; DOMINGO-FERRER, J. Big Data Privacy: Challenges to Privacy Principles and Models. **Data Science and Engineering**, v. 1, p. 21-28, 2016. Disponível em: https://link.springer.com/content/pdf/10.1007/s41019-015-0001-x.pdf. Acesso em 1 mar. 2021.

TALHA, M.; KALAM, A.; ELMARZOUQI, N. Big Data: Trade-off between Data Quality and Data Security. **Procedia Computer Science**, v 151, p. 916-922, 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050919305915. Acesso em: 20 mar. 2021.

TCU - TRIBUNAL DE CONTAS DA UNIÃO. **Referencial básico de governança aplicável a órgãos e entidades da administração pública**. Versão 2, 2014. Disponível em: https://portal.tcu.gov.br/data/files/E8/14/13/3D/43B0F410E827A0F42A2818A8/2663788.PDF. Acesso em: 15 mar. 2021.

THOMPSON, N.; RAVINDRAN, R.; NICOSIA, S. Government data does not mean *Data Governance*: Lessons learned from a public sector application audit. **Government Information Quarterly**, v. 32, n. 3, p. 316-322, 2015. Disponível em: https://www.sciencedirect.com/science/article/pii/S0740624X15000593. Acesso em: 05 mar. 2021.

TORRA, V.; NAVARRO-ARRIBAS, G. Data privacy. **WIREs Data Mining Knowledge Discovery**, v. 4, p. 269-280, 2014. Disponível em: https://doi.org/10.1002/widm.1129. Acesso em: 22 fev. 2021.

VENTURA, M.; COELI, C. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. **Cad. Saúde Pública**, Rio de Janeiro, v. 34, n. 7, mai. 2018. Disponível em: http://cadernos.ensp.fiocruz.br/csp/artigo/486/para-alem-da-privacidade-direito-a-informacao-na-saude-protecao-de-dados-pessoais-e-governanca. Acesso em: 15 mar. 2021.

Felipe Fonseca Salerno
Mestre em Social Statistics pela University of Glasgow (Escócia), Estatístico no Tribunal de Justiça do Rio Grande do Sul.

Antônio Carlos Gastaud Maçada
Mestre e Doutor em Administração pela Universidade Federal do Rio Grande do Sul (UFRGS), Brasil, Professor Titular da Escola de Administração da UFRGS e Bolsista de Produtividade 1C CNPq.