

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E EXTENSÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL
PROJETO DE PESQUISA: DEMOCRACIA, PROCESSO E JURISDIÇÃO

**GOVERNANÇA DIGITAL NO PODER JUDICIÁRIO DE
SANTA CATARINA: UMA ANÁLISE SOBRE A
POSSIBILIDADE DE UTILIZAÇÃO DA *BLOCKCHAIN* EM
SISTEMAS DO PJSC**

VICTOR ANTONIO CECYN

Itajaí-SC, dezembro de 2024

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E EXTENSÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL
PROJETO DE PESQUISA: DEMOCRACIA, PROCESSO E JURISDIÇÃO

**GOVERNANÇA DIGITAL NO PODER JUDICIÁRIO DE
SANTA CATARINA: UMA ANÁLISE SOBRE A
POSSIBILIDADE DE UTILIZAÇÃO DA *BLOCKCHAIN* EM
SISTEMAS DO PJSC**

VICTOR ANTONIO CECYN

Dissertação submetida ao Curso de Mestrado em
Ciência Jurídica da Universidade do Vale do Itajaí –
UNIVALI, como requisito parcial à obtenção do título
de Mestre em Ciência Jurídica.

Orientadora: Professora Doutora Luciene Dal Ri

Itajaí-SC, dezembro de 2024

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais Calixto e Elenita, alicerces desta jornada dos quais sempre se sacrificaram e me motivaram.

À minha companheira Rafaela, pelo apoio incondicional e presença encorajadora.

À minha orientadora e amiga, Profa. Doutora Luciene Dal Ri, por todas as oportunidades e ensinamentos que pude receber.

Ao Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica (PPCJ) - Curso de Mestrado em Ciência Jurídica (CMCJ), da Universidade do Vale do Itajaí-UNIVALI e, em especial, a todos os docentes e colegas.

Ao Programa de Pós-Graduação Stricto Sensu – Mestrado em Direito, da Universidade Federal de Santa Catarina – UFSC, que me proporcionou aprofundar esta pesquisa e ampliar minha visão por meio das disciplinas cursadas nesta instituição.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pela bolsa que financiou meus estudos.



- Fundação da Casa do Estudante e Escritório-Modelo de Advocacia (1972)¹.

Em memória de meu Avô, Calixto Antonio Cecyn.

¹ Acervo histórico da Universidade do Vale do Itajaí – UNIVALI.

- Quando vocês acham que as pessoas morrem?
 - Quando uma bala perfura seu coração!?
 - Não.
- Quando são vencidas por uma doença incurável?
 - Não.
 - Elas morrem quando são esquecidas.

Dr. Hiluluk

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca deste trabalho.

Itajaí-SC, dezembro de 2024



Documento assinado digitalmente

VICTOR ANTONIO CECYN

Data: 29/07/2025 16:42:35-0300

Verifique em <https://validar.iti.gov.br>

**Victor Antonio Cecyn
Mestrando**



UNIVERSIDADE DO VALE DO ITAJAÍ

PÁGINA DE APROVAÇÃO

Conforme Ata da Banca de defesa de Mestrado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica PPCJ/UNIVALI, em 17 de dezembro de 2024, às dez horas, por meio remoto pela plataforma Microsoft Teams o mestrando **Victor Antonio Cecyn**, fez a apresentação e defesa da Dissertação, sob o título sob título **“Governança digital no poder judiciário de Santa Catarina: uma análise sobre a possibilidade de utilização da blockchain em sistemas do PJSC”**.

A Banca Examinadora foi formada mediante o Ato Organizacional número 098/PPCJ/2024, baixado pelo Coordenador do Programa Pós-Graduação *Stricto Sensu* em Ciência Jurídica, Professor Doutor Paulo Márcio da Cruz, composta pelos Professores, Doutora Luciene Dal Ri (UNIVALI), como presidente e orientadora, Doutor Cláudio Carneiro Bezerra Pinto Coelho (Faculdade de Guanambi/BA), como membro, Doutor Clovis Demarchi (UNIVALI), como membro, Doutora Helena Schiessl Cardoso (Pós-Doutorado UNIVALI), como membro suplente. Por motivos de saúde, do membro Doutor Cláudio Carneiro Bezerra Pinto Coelho, participou da banca a suplente, professora Doutora Helena Schiessl Cardoso.

Conforme consta em Ata, após a avaliação dos membros da Banca, a Dissertação foi aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), 17 de dezembro de 2024.

Prof. Dr. Paulo Márcio Da Cruz
Coordenador/PPCJ/UNIVALI

ROL DE ABREVIATURAS E SIGLAS

ANS	Acordo de Nível de Serviço
CGeproc	Comitê Gestor do eproc
CGESTI	Comitê Gestor de Tecnologia da Informação
CGovTI	Comitê de Governança de Tecnologia da Informação
CNJ	Conselho Nacional de Justiça
DAGG	Divisão de Apoio à Gestão e Governança de TI
DITI	Divisão de Infraestrutura de TI
DRC	Divisão de Redes de Comunicação
DSA	Divisão de Sistemas Administrativos
DSGA	Divisão de Suporte e Gestão de Ativos de TI
DSJ	Divisão de Sistemas Judiciais
DTI	Diretoria de Tecnologia da Informação
ENTIC-JUD	Estratégia Nacional do Poder Judiciário
eproc	Processo Judicial Eletrônico
IA	Inteligência Artificial
LDO	Lei de Diretrizes Orçamentárias
LOA	Lei Orçamentária Anual
LRF	Lei de Responsabilidade Fiscal

MNI	Modelo Nacional de Interoperabilidade
NCI	Núcleo de Comunicação Institucional
NUGEPNAC	Núcleo de Gerenciamento de Precedentes e de Ações Coletivas
NUMOPEDE	Núcleo de Monitoramento de Perfil de Demandas e Estatística
PCE	Prestação de Contas Extrajudiciais
PCTIC	Plano de Contratações de Tecnologia da Informação e Comunicação
PDTI	Plano Diretor de Tecnologia da Informação
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PEI	Planejamento Estratégico Institucional
PJSC	Poder Judiciário do Estado de Santa Catarina
PPA	Plano Plurianual
SAJ	Sistema de Automação da Justiça
SCE	Sistema de Cadastro do Extrajudicial
SCT	Sistema de Controle de Custos
SEEU	Sistema Eletrônico de Execução Unificado
SSIGR	Secretaria de Segurança da Informação e Gestão de Riscos de TI

TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TJSC	Tribunal de Justiça de Santa Catarina

LISTA DE FIGURAS

Figura 1 – Exemplo de “Nós” em redes centralizadas e descentralizadas.....	66
Figura 2 – Exemplo de auditabilidade em logs de registro.....	68

LISTA DE TABELAS

Tabela 1 – Objetivos da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário.....	44
Tabela 2 – Diretrizes e Estratégias de Tecnologia da Informação.....	48
Tabela 3 – Princípios PDTIC PJSC.....	54
Tabela 4 – Projetos priorizados CGovTI.....	56

LISTA DE GRÁFICOS

Gráfico 1 – Orçamento Tecnologia da Informação PJSC 2019.....	50
Gráfico 2 – Orçamento Tecnologia da Informação PJSC 2020.....	51
Gráfico 3 – Orçamento Tecnologia da Informação PJSC 2021.....	51
Gráfico 4 – Orçamento Tecnologia da Informação PJSC 2022.....	52
Gráfico 5 – Orçamento Tecnologia da Informação PJSC 2023.....	52
Gráfico 6 – Orçamento Tecnologia da Informação PJSC 2024.....	52
Gráfico 7 – Resultado IGOVTICJUD 2016-2020.....	60
Gráfico 8 – Resultado IGOVTICJUD 2023.....	61
Gráfico 9 – Índice Pontuação IGOVTICJUD 2016-2020.....	102
Gráfico 10 – Índice Pontuação IGOVTICJUD 2021-2024.....	102

ROL DE CATEGORIAS

Agenda 2030: É uma agenda global de desenvolvimento sustentável adotada pelas Nações Unidas em 2015. Ela consiste em um conjunto de 17 Objetivos de Desenvolvimento Sustentável (ODS) que abrangem áreas como erradicação da pobreza, igualdade de gênero, ação climática, educação de qualidade, entre outros. A Agenda 2030 tem como objetivo principal promover a paz, a prosperidade e o bem-estar das pessoas, garantindo a proteção do meio ambiente².

Auditabilidade: Refere-se à possibilidade de auditar os sistemas para garantir a transparência, responsabilização e conformidade com padrões éticos e legais. É a capacidade de examinar e verificar os processos e resultados dos algoritmos de IA para garantir sua adequação e evitar vieses e discriminação³.

Big Data: Refere-se a conjuntos de dados complexos e de difícil interpretação, que não podem ser processados por meio de ferramentas de banco de dados convencionais. O Big Data é caracterizado por grandes volumes, variedade de formatos e velocidade de geração. É utilizado para extrair insights e obter uma visão detalhada de subcategorias e submercados que amostragens menores não alcançam⁴.

Blockchain: tecnologia inserida em software que realiza duas ações: verificação rápida de modificação nos dados e correção automática com base em replicadores desses dados. Com isso gera-se a imutabilidade dos dados, não permitindo a modificação de conteúdo que lhe foi inserido⁵.

Criptografia: A origem da palavra criptografia deriva das palavras gregas κρυπτός (kryptos), que significa escondido, e γράφειν (grafein), que significa escrever.

² ONU. Organização das Nações Unidas. Transformando Nosso Mundo: A Agenda 2030 para o Desenvolvimento Sustentável. 2015. Disponível em: <https://nacoesunidas.org/wpcontent/uploads/2015/10/agenda2030-pt-br.pdf> > Acesso em 01.nov.2024.

³ LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008. 253 p.

⁴ SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1a ed. São Paulo: Edipro, 2016.

⁵ LAGO, Lucas. **Blockchain: confiança através de algoritmos**. Escola Politécnica do Estado de São Paulo, CEST – Boletim, v. 2, n. 4. out. 2017. p. 1.

Representava, inicialmente, uma forma diferente de escrita, que buscava impossibilitar a compreensão de mensagens trocadas, como uma espécie de “falar em códigos”, isto é, a forma não corresponde com a mensagem enviada, portanto, incompreendida, o que garantia a segurança das informações trocadas. Pela criptografia, uma mensagem simples é transformada numa mensagem cifrada, decifrada apenas por uma ou mais chaves. A criptografia é um método de codificação de dados que permite o acesso apenas de pessoas autorizadas, que possuem uma chave de acesso⁶.

Dados Pessoais: É a informação relacionada a pessoa identificada ou identificável, sendo um dado é considerado pessoal quando ele permite a identificação, direta ou indireta, da pessoa física por trás do dado.

Dados Pessoais Sensíveis: são aqueles dados que podem causar discriminação a uma pessoa, por isso merecem maior proteção, tais como dos dados relacionados à origem racial/étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético/ biométrico⁷.

General Data Protection Regulation (GDPR): O Regulamento UE 2016/679 da União Europeia é a norma que esclarece como dados pessoais devem ser legalmente tratados incluindo como devem ser coletados, usados, protegidos ou compartilhados em geral. Fortalece a proteção de dados para todas as pessoas cujas informações pessoais se enquadram em seu escopo, dando-lhes o controle total de seus dados pessoais⁸.

⁶ EDGE, Charles; O'DONNELL, Daniel. **Introduction to cryptography**. In: LOPES, Marcus Vinícius Pimenta. A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de provas digitais. Tese de Doutorado. 218 f. Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023. p. 73

⁷ 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 05 mai. de 2023.

⁸ UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 26 Set 2023.

Lei Geral de Proteção de Dados Pessoais (LGPD): A Lei nº 13.709/2018 foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais⁹.

⁹ 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 05 mai. de 2023.

SUMÁRIO

RESUMO.....	10
RESUMEN	11
INTRODUÇÃO	12
Capítulo 1	18
SUJEITOS DE DIREITOS EM UMA SOCIEDADE GLOBALIZADA .	18
1.1 SOCIEDADE DA INFORMAÇÃO, ECONOMIA DE DADOS E REVOLUÇÕES INDUSTRIAIS	18
1.1.1 Evolução Histórica da Tutela Jurisdicional Acerca da Proteção e Privacidade de Dados no Contexto Europeu e Brasileiro	21
1.1.2.1. <i>A Importância da Governança Digital em um ordenamento que tutela a proteção e privacidade de dados como direito fundamental</i>	27
1.1.2.2. <i>Conceituando “governança digital” sob o viés da administração pública</i>	31
1.1.2.3. <i>Contornos Jurídicos: Situando a governança digital no ordenamento jurídico brasileiro</i>	33
1.1.2.4. <i>O Decreto 9.319/2018 - Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital</i>	34
1.1.2.5. <i>Decreto 10.322/2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências</i>	37
1.1.2.6. <i>Decreto 10.222/2020 – Estratégia Nacional de Segurança Cibernética</i>	39
1.1.2.7. <i>Desafios da Governança Digital – Comitês Gestores</i>	42
1.2 ASCENSÃO DO PROGRAMA DE GOVERNANÇA DIGITAL NO PJSC	44
1.2.1 PLANO ORÇAMENTÁRIO	50
1.2.2 PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	54
1.2.3 LEVANTAMENTO DE GOVERNANÇA, GESTÃO E INFRAESTRUTURA DE TIC DO PJSC.....	59
Capítulo 2	63
A UTILIZAÇÃO DE <i>BLOCKCHAIN</i> COMO MEDIDA DE PREVENÇÃO À INCIDENTES DE SEGURANÇA	63

2.1 ENTENDENDO A OPERACIONALIZAÇÃO DA <i>BLOCKCHAIN</i>	63
2.2 BENEFÍCIOS DA APLICAÇÃO DA <i>BLOCKCHAIN</i>	67
2.2.1 Auditoria de Eventos.....	68
2.2.2 Contratos Inteligentes (<i>Smart Contracts</i>)	71
2.2.3 Gerenciamento de Acessos	73
2.2.4 Serviços de Tradução de Provas Estrangeiras	74
2.2.5 Depósito Eletrônico de Dados de Direitos Autorais.....	77
2.3 DESAFIOS ESPERADOS.....	79
2.3.1 Legislação	79
2.3.2 Operação Técnica	81
2.3.3 Cultura Organizacional	83
2.3.4 Investimento	84
Capítulo 3	85
ANALISANDO TRIBUNAIS NACIONAIS E INTERNACIONAIS.....	85
3.1 IMPLEMENTAÇÕES DE <i>BLOCKCHAIN</i> NO JUDICIÁRIO BRASILEIRO....	85
3.1.1 Tribunal de Contas da União.....	85
3.1.2 Tribunal de Justiça do Maranhão	86
3.1.3 Tribunal de Justiça do Rio Grande do Sul	87
3.1.4 Conselho Nacional de Justiça.....	88
3.2 INICIATIVAS DA TECNOLOGIA <i>BLOCKCHAIN</i> EM OUTROS PAÍSES	90
3.2.1 África do Sul	90
3.2.2 Estônia	92
3.2.3 Malta	93
3.2.4 Emirados Árabes Unidos (Dubai).....	94
3.2.5 Estados Unidos da América	95
3.2.6 Rússia.....	99
3.3 PERSPECTIVAS PARA A GOVERNANÇA DIGITAL NO PJSC: AVANÇOS, DESAFIOS E A INTEGRAÇÃO DO <i>BLOCKCHAIN</i>	99
CONSIDERAÇÕES FINAIS	107
REFERÊNCIA DAS FONTES CITADAS.....	115

RESUMO

A Dissertação está inserida na Área de Concentração Fundamentos do Direito Positivo, sob a Linha de Pesquisa Direito, Jurisdição e Inteligência Artificial e o projeto de pesquisa Democracia, Processo e Jurisdição. O objetivo institucional da presente dissertação é a obtenção do título de Mestre em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali. Tem como objetivo geral a análise da maturidade do programa de governança digital presente no Poder Judiciário de Santa Catarina (PJSC), desde o ano de 2018, marco temporal que deu início à atividade de análise da maturidade do programa, a fim de compreender os riscos atrelados à utilização dos atuais procedimentos administrativos internos e ferramentas tecnológicas para execução mesmos e, a partir deste levantamento, em caráter específico, verificar se a utilização do *blockchain* se reverte em uma medida de combate aos riscos cibernéticos e de cumprimento da proteção e privacidade de dados e demais direitos dos titulares elencados na Constituição Federal e Lei.13.709/2018. Para alcançá-lo, foram traçados os objetivos específicos que compreendem os capítulos 1, 2 e 3, os quais tratam respectivamente do estudo histórico acerca do desenvolvimento desenfreado de tecnologias e de revoluções industriais, assim como do programa de governança digital do PJSC e a inserção do mesmo no ordenamento jurídico brasileiro; análise da tecnologia de *blockchain* e a possibilidade de aplicação da mesma em atividades dos órgãos do judiciário; e estudos de caso sobre a aplicação da *blockchain* em tribunais nacionais, assim como em governos internacionais. Nas considerações finais, restou demonstrado que no âmbito tecnológico, a *blockchain* representa uma das soluções mais inovadoras e promissoras da atualidade, com um vasto potencial de aplicação no setor público. Sua capacidade de assegurar a integridade dos dados, garantir auditorias seguras e promover a interoperabilidade entre diferentes sistemas administrativos e judiciais pode revolucionar a forma como o Judiciário opera. Além disso, ao promover a transparência e a eficiência, a *blockchain* pode ser um catalisador para a transformação digital de outras áreas do governo, criando um efeito dominó que pode beneficiar todo o setor público brasileiro. A implantação de uma solução tecnológica tão avançada também abre portas para novos investimentos e parcerias público-privadas no desenvolvimento de soluções digitais que beneficiem tanto o governo quanto os cidadãos. A pesquisa está envolta do Objetivo de Desenvolvimento Sustentável – ODS de número 16, da Agenda 2030 da Organização das Nações Unidas – ONU, qual seja, a missão de 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. O trabalho utilizou os Métodos Indutivos e Cartesiano e a base lógica indutiva no Relatório dos Resultados, bem como na pesquisa as Técnicas do Referente, da Categoria, do Conceito Operacional e da Pesquisa Bibliográfica.

Palavras-chave: *Blockchain*; Governança Digital; Poder Judiciário de Santa Catarina; Proteção e Privacidade de Dados; Segurança da Informação.

RESUMEN

La Disertación está inserta en el Área de Concentración Fundamentos del Derecho Positivo, bajo la Línea de Investigación Derecho, Jurisdicción e Inteligencia Artificial y el proyecto de investigación Democracia, Proceso y Jurisdicción. El objetivo institucional de esta disertación es la obtención del título de Maestro en Ciencia Jurídica por el Curso de Maestría en Ciencia Jurídica de Univali. Tiene como objetivo general el análisis de la madurez del programa de gobernanza digital presente en el Poder Judicial de Santa Catarina (PJSC) desde el año 2018, marco temporal que dio inicio a la actividad de análisis de la madurez del programa, con el fin de comprender los riesgos asociados a la utilización de los actuales procedimientos administrativos internos y herramientas tecnológicas para su ejecución. A partir de este levantamiento, de manera específica, se busca verificar si la utilización de *blockchain* se traduce en una medida para combatir los riesgos cibernéticos y garantizar la protección y privacidad de datos, así como otros derechos de los titulares establecidos en la Constitución Federal y la Ley 13.709/2018. Para lograrlo, se establecieron los objetivos específicos que comprenden los capítulos 1, 2 y 3, los cuales tratan, respectivamente, del estudio histórico sobre el desarrollo desenfrenado de tecnologías y revoluciones industriales, así como del programa de gobernanza digital del PJSC y su inserción en el ordenamiento jurídico brasileño; el análisis de la tecnología *blockchain* y la posibilidad de su aplicación en las actividades de los órganos del poder judicial; y estudios de caso sobre la aplicación de *blockchain* en tribunales nacionales, así como en gobiernos internacionales. En las consideraciones finales, se demostró que en el ámbito tecnológico, *blockchain* representa una de las soluciones más innovadoras y prometedoras de la actualidad, con un vasto potencial de aplicación en el sector público. Su capacidad para asegurar la integridad de los datos, garantizar auditorías seguras y promover la interoperabilidad entre diferentes sistemas administrativos y judiciales puede revolucionar la forma en que opera el Poder Judicial. Además, al promover la transparencia y la eficiencia, *blockchain* puede ser un catalizador para la transformación digital de otras áreas del gobierno, creando un efecto dominó que puede beneficiar a todo el sector público brasileño. La implementación de una solución tecnológica tan avanzada también abre puertas a nuevas inversiones y asociaciones público-privadas en el desarrollo de soluciones digitales que benefician tanto al gobierno como a los ciudadanos. La investigación está enmarcada en el Objetivo de Desarrollo Sostenible – ODS número 16 de la Agenda 2030 de la Organización de las Naciones Unidas – ONU, que tiene como misión promover sociedades pacíficas e inclusivas para el desarrollo sostenible, proporcionar acceso a la justicia para todos y construir instituciones eficaces, responsables e inclusivas en todos los niveles. El trabajo utilizó los Métodos Inductivos y Cartesianos y la base lógica inductiva en el Informe de Resultados, así como las Técnicas del Referente, de la Categoría, del Concepto Operacional y de la Investigación Bibliográfica.

Palabras clave: *Blockchain*; Gobernanza Digital; Poder Judicial de Santa Catarina; Protección y Privacidad de Datos; Seguridad de la Información.

INTRODUÇÃO

A Dissertação está inserida na Área de Concentração Fundamentos do Direito Positivo, sob a Linha de Pesquisa Direito, Jurisdição e Inteligência Artificial e o projeto de pesquisa Democracia, Processo e Jurisdição.

O objetivo institucional da presente dissertação é a obtenção do título de Mestre em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali.

Quanto ao objetivo investigatório, este resume-se na análise da maturidade do programa de governança digital presente no Poder Judiciário de Santa Catarina (PJSC), a fim de compreender os riscos atrelados à utilização dos atuais procedimentos administrativos internos e ferramentas tecnológicas para execução mesmos e, a partir deste levantamento, em caráter específico, verificar se a utilização do *blockchain* se reverte em uma medida de combate aos riscos cibernéticos e de cumprimento da proteção e privacidade de dados e demais direitos dos titulares elencados na Constituição Federal e Lei.13.709/2018.

Ao mesmo tempo em que, de um lado, a proteção de dados eleva-se ao patamar de direito fundamental resguardado pelo texto constitucional brasileiro, por outro lado, o globo transita por um tortuoso período de insegurança frente aos meios digitais na nova sociedade da informação.

Claro exemplo que traz relevância à temática é o ataque cibernético sofrido pelo Superior Tribunal de Justiça¹⁰ em 03/11/2020, o qual foi considerado o maior incidente em face de instituição judiciária brasileira até então, de forma que toda a operacionalização das demandas judiciais foi suspensa e o restabelecimento da distribuição de processos ocorreu apenas 168 horas após o ocorrido, levando-se em conta uma extensa força tarefa montada para responder o incidente.

¹⁰ SUPERIOR TRIBUNAL DE JUSTIÇA. **Comunicado da Presidência do STJ**. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em 10 de mai. 2022.

Todavia, os incidentes não cessaram neste fatídico episódio, diversos ataques hackers vêm sendo disferidos contra órgãos do judiciário, dentre eles destacam-se eventos ocorridos nos sistemas do TJRS¹¹, TSE¹² e TRF¹³.

Outro ponto relevante para o tema está respaldado em um estudo realizado pela União Internacional de Telecomunicações, órgão da ONU, o qual apontou que o Brasil foi o 2º país de todo o globo que mais sofreu prejuízos de ordem econômica decorrentes de ataques cibernéticos no ano de 2019, com fulcro ao disposto pelo Senado¹⁴.

Diante disso, esta dissertação tem o condão de levantar os riscos cibernéticos e regulatórios no que diz respeito aos atuais programas de governança e compliance digital do Poder Judiciário de Santa Catarina, assim como elencar e propor parâmetros de implementação e aplicação de *blockchain* em prol da contínua melhoria da prestação da efetiva tutela jurisdicional prestada pelo PJSC em reflexo aos cidadãos.

Assim, será possível medir um nível de aderência/maturidade ao compliance digital presente na estrutura de governança do PJSC, confrontada por meio de dados coletados pelo Conselho Nacional de Justiça. A pesquisa compreende ainda a análise bibliográfica e documental disponibilizada pelo PJSC até o momento, no que diz respeito à implementação, administração e desenvolvimento dos sistemas judiciais e governança digital presente no programa institucional do Órgão.

¹¹ TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. **Nota de esclarecimento**. Disponível em: <https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/>. Acesso em: 05 de mai. 2022.

¹² TRIBUNAL SUPERIOR ELEITORAL. **TSE institui comissão presidida por Alexandre e Moraes para acompanhar investigações sobre ação de hackers contra o processo eleitoral**. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2020/Novembro/tse-institui-comissao-presidida-por-alexandre-de-moraes-para-acompanhar-investigacoes-sobre-acao-de-hackers-contr-o-processo-eleitoral?SearchableText=HACKER>. Acesso em: 05 de mai. 2022.

¹³ CNN. **Sob suspeita de ataque hacker, TRF-1 blinda sistema eletrônico**. Disponível em: <https://www.cnnbrasil.com.br/nacional/sob-suspeita-de-ataque-hacker-trf-1-blinda-sistema-eletronico/>. Acesso em: 05 de mai. 2022.

¹⁴ SENADO NOTÍCIAS. **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>. Acesso em: 10 de mai. 2022.

Após o levantamento de informações e diretrizes aplicáveis ao atual modelo de gestão marcado pela descentralização de sistemas, realizar-se-á uma avaliação acerca da eficiência na aplicação da tecnologia *blockchain*, a fim de que, ao final, haja a possibilidade de propor melhorias ao programas de governança digital do PJSC e, conseqüentemente, o fator benéfico na busca da efetiva garantia da tutela de direitos fundamentais dos titulares de dados envolvidos nas atividades de tratamento do referido órgão.

Para a pesquisa, foram levantados os seguintes problemas:

- a) O atual programa de governança digital do PJSC respalda-se em um projeto estruturado e em contínua melhoria? O programa corresponde à eficaz tutela de direitos fundamentais dos cidadãos, ou os põe em risco?
- b) Diante deste cenário, a aplicação da *blockchain* mostra-se uma medida viável para elevar a maturidade do programa de governança digital do PJSC?

Diante dos problemas levantados, apresentaram-se as seguintes hipóteses:

- a) Espera-se a localização de diversas ações de melhoria necessárias ao programa de governança digital do PJSC, melhorias das quais ressoarão em: a) maior aderência ao cumprimento legal e tutela do direito fundamental garantido pela Constituição Federal à massiva quantidade de indivíduos envolvidos nas operações de tratamento de dados do PJSC; b) desenvolvimento e alçada da maturidade do programa de Compliance Digital e; c) a mitigação de ameaças cibernéticas a partir da inibição dos riscos levantados e a consequente proteção do patrimônio do PJSC, tanto no que se refere à reputação do órgão e montante econômico presente no ativo informacional detido pelo mesmo, quanto no amortecimento de gastos decorrentes de incidentes de segurança e vazamentos de dados, os quais se provaram exorbitantes e complexos.
- b) Acredita-se que a aplicação da tecnologia de *blockchain* em inclusão ao pilar de segurança da informação do programa de governança favorece a concretização do ODS16 na promoção de sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionando o acesso à justiça para todos e construindo instituições eficazes, responsáveis e inclusivas em todos os níveis.

Visando pesquisar as hipóteses propostas, a dissertação foi dividida em três capítulos, quais sejam:

No capítulo 1, faz-se uma inserção do contexto histórico acerca do desenvolvimento desenfreado de tecnologias e de revoluções industriais das quais quebraram paradigmas frente a forma da qual se apresentava a sociedade. Aborda-se também a evolução histórica de adoção da privacidade e da proteção de dados na qualidade de direitos positivados por Estados globais, em um primeiro momento, bem como na conseguinte adoção por parte do ordenamento jurídico brasileiro.

Deste modo, expõe-se o debate doutrinário acerca da conceituação do termo “governança digital”, assim como da importância de sua implementação e contínua melhoria frente ao contexto tecnológico marcado por inseguranças e exploração de fragilidades virtuais que ameaçam direitos fundamentais.

Por fim, busca-se expor o contexto legislativo dos programas de governança digital inseridos na administração pública e, em especial, nos órgãos do poder judiciário, afunilando-se ainda em uma análise do atual programa de governança digital do PJSC e seus resultados frente aos marcadores estabelecidos pelo Conselho Nacional de Justiça.

O Capítulo 2 trata da conceituação da tecnologia *blockchain* e, respectivamente, da operacionalização da tecnologia da qual recebe destaque mundial e ascende-se primariamente no setor bancário, muito marcado por sua inclusão em transações entre criptomoedas. Ademais, apresentam-se os desafios esperados em equilíbrio às janelas de oportunidade das quais são atualmente utilizadas em decorrência da aplicação da *blockchain* em cenários concretos.

Portanto, no capítulo 3 empreende-se uma exposição de tribunais nacionais dos quais exploram formas de implementação da *blockchain* e internalização da tecnologia em seus programas de governança digital.

Além disso, propõe-se o estudo e análise dos grandes casos de sucesso em governos e tribunais internacionais pioneiros na implementação da *blockchain* em seu cotidiano operacional, assim como da utilização da tecnologia para fins diversos

dos quais eram projetados inicialmente, quais sejam, a tokenização de ativos financeiros.

A Dissertação se encerra com as considerações finais, nas quais são apresentados aspectos destacados da dissertação, seguidos de estimulação à continuidade dos estudos e das reflexões sobre o atual programa de governança digital do PJSC e a possibilidade de utilização da *blockchain* como medida de proteção de direitos fundamentais e prevenção de incidentes de segurança.

Quanto à Metodologia empregada, registra-se que, na Fase de Investigação¹⁵ foi utilizado o Método Indutivo¹⁶ em razão da coleta de informações que fundaram a percepção geral e oportunizaram a conclusão, conforme observado no capítulo 1 e 2, o procedimento Cartesiano¹⁷ na Fase de Tratamento de Dados composta pela análise de dados obtidos a partir da maturidade do programa de governança digital do PJSC e nos estudos de caso presentes no capítulo 3, e, o Relatório dos Resultados expresso na presente Dissertação é composto na base lógica indutiva.

Nas diversas fases da Pesquisa, foram acionadas as Técnicas do Referente¹⁸, da Categoria¹⁹, do Conceito Operacional²⁰ e da Pesquisa Bibliográfica²¹.

¹⁵ “(...) momento no qual o Pesquisador busca e recolhe os dados, sob a moldura do Referente estabelecido (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018. p. 112-113.

¹⁶ “(...) pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 114.

¹⁷ Sobre as quatro regras do Método Cartesiano (evidência, dividir, ordenar e avaliar) veja LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001. p. 22-26.

¹⁸ “(...) explicitação prévia do(s) motivo(s), do(s) objetivo(s) e do produto desejado, delimitando o alcance temático e de abordagem para a atividade intelectual, especialmente para uma pesquisa.” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 69.

¹⁹ “(...) palavra ou expressão estratégica à elaboração e/ou à expressão de uma ideia.” PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 41.

²⁰ “(...) uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideias que expomos (...)”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 58.

²¹ “Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais”. PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. p. 217.

Informo ainda que a pesquisa foi realizada mediante apoio financeiro do Programa de Excelência Acadêmica regulado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

Capítulo 1

SUJEITOS DE DIREITOS EM UMA SOCIEDADE GLOBALIZADA

1.1 SOCIEDADE DA INFORMAÇÃO, ECONOMIA DE DADOS E REVOLUÇÕES INDUSTRIAIS

A sociedade sofreu grandes rupturas em sua organização estrutural ao longo do tempo, de forma que em cada período um elemento foi essencial para a ocorrência da quebra de paradigmas, por conta desta estruturação os elementos se tornaram marcos históricos, conforme retrata Silva²².

O primeiro marco da linha temporal estudada resume-se na chamada Primeira Revolução Industrial que começou na região da Grã-Bretanha por volta do século XVIII por meio de uma grande disrupção da economia agrária que neste novo momento contara com métodos de produção mecânicos, destacando-se a construção de ferrovias e máquinas movidas a vapor.

O próximo período é marcado por um rompimento ainda mais brusco, abarcado pelo desenvolvimento do motor a combustão, utilização de petróleo como fonte de combustível, a chegada da produção em escala industrial facilitada em razão da energia elétrica e por conta das linhas de produção contínuas e em massa, marcando assim a Segunda Revolução Industrial no final do século XIX.

A chegada da microeletrônica e da Tecnologia da Informação no processo industrial marca o início de um longo período da sociedade globalizada, marcada por produções otimizadas e automatizadas no fim da década de 1960, fato que compreende a Terceira Revolução Industrial, conforme entendem Drath e Horch²³.

²² SILVA, Daniel Pereira Militão. **Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação**. Dissertação (Mestrado) – Faculdade de Direito da Pontifícia Universidade Católica de São Paulo. São Paulo, 2009.

²³ DRATH, Rainer, HORCH, Alexander. Industrie 4.0: Hit or Hype? [Industry Forum]. IEEE **Industrial Electronics Magazine**, [S.l.] v.8, n. 2, p. 56-58, 2014. DOI: 10.1109/MIE. 2014.2312079. Disponível em:

Na visão de Klaus Schwab²⁴, compreender a nova revolução tecnológica surgida, revertida na Quarta Revolução Industrial, tornou-se o maior desafio da sociedade, pois as mudanças incorridas pelo mencionado movimento vão além da quebra de atuais referências sobre a forma de executar atividades laborais e comunicar-se entre indivíduos, mas também abrangem a reorganização de governos e instituições, fator que impacta consequentemente o PJSC e se instaura como marco teórico do presente estudo.

Noutro ponto, torna-se imperioso destacar o cenário de uma globalização acelerada essencial para a transformação do mercado, esta provida por meio de tecnologias da informação e comunicação, em razão disso há o surgimento de novas ferramentas aplicáveis ao processo industrial, tais como automatização e digitalização de processos e serviços, análise de *big data*, *softwares* incorporados, sistema de comunicação e rede (sistemas em nuvem), sistemas integrados embarcados, robôs autônomos, inteligência artificial e entre outros concebem o termo “indústria 4.0”, insurgido primariamente por parte do governo alemão na Feira de Hannover, em 2011, revertendo-se no marco da Quarta Revolução Industrial, consonante com Salkin²⁵.

Veja-se, a Quarta Revolução não se resume ao advento da internet, *world wide web*, criada em 1992²⁶, apesar da Terceira Revolução Industrial contar com o surgimento de tecnologias, a grande diferença para o salto da Quarta Revolução é marcada por tecnologias com rápida capacidade de evolução e um crescimento exacerbado evidente, destacada desta forma como a “segunda era da máquina” por Erik Brynjolfsson e Andrew McAfee²⁷, as novas máquinas elevam a sociedade humana

<http://ieeexplore.ieee.org/document/6839101/>. Acesso em: 09 mai. 2024.

²⁴ SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1a ed. São Paulo: Edipro, 2016.

²⁵ SALKIN, Ceren; ONER, Mahir; USTUNDAG, Alp; CEVIKCAN, Emre. A Conceptual Framework for Industry 4.0. In: USTUNDAG, Alp; CEVIKCA, Emre (org.). **Industry 4.0: Managing The Digital Transformation**. Cham: Springer International Publishing, 2018. DOI: 10.1007/9783319578705_1. Disponível em: http://link.springer.com/10.1007/9783319578705_1, Acesso em: 09 mai. 2024.

²⁶ ROSA, Alexandre de Moraes; GARCIA, Lara Rocha; PINTO, Felipe Chiarello de Souza. **Direito para Humanos Robotizados ou Direito dos Robôs Humanizados?** REVISTA NOVOS ESTUDOS JURÍDICOS -ELETRÔNICA, VOL. 28 -N. 3. Disponível em: <https://periodicos.univali.br/index.php/nej/article/view/19985/11614>.

²⁷ BRYNJOLFSSON, Erik; MCAFFE, Andrew. **The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies**, W Norton & Company, 2014.

a outro patamar, de forma que influenciam neste momento o próprio pensamento humano e sua compreensão, não se limitando à mudança de um modelo de produção econômico e desbravando-se em novos campos de interação do indivíduo.

O atual modelo organizacional da sociedade gira em torno de “informações”, consonante com Bioni²⁸, a título de elemento essencial para o desenvolvimento da economia, matéria que substituiu os antigos proventos que estruturam as revoluções industriais, quais sejam a agrícola, a industrial e a pós-industrial.

Os relacionamentos sociais transmutados na visão de Schwab²⁹ foram submersos em fluxos informacionais de dados processados a velocidades de modo algum antes vistas, considerando que neste momento não há quaisquer obstáculos físicos em razão da distância ou escalabilidade, fato que também mudou a forma como os indivíduos compreendem o conceito entre tempo-espaço.

Os novos e inimagináveis parâmetros computacionais de processamento de dados consequentemente desembocaram no rápido desenvolvimento das formas de coletar, armazenar e tratar dados, ciclo histórico marcado pelos termos *Big Data*, Internet das Coisas e Inteligência Artificial, resumido por tecnologias que possibilitaram a automatização de ações e processamento de dados e fundamentaram a nomenclatura de uma “economia de dados”³⁰.

Neste sentido, Schwab³¹ destaca três pilares que fundamentam a insurgência de uma nova Revolução Industrial, quais sejam, a velocidade exacerbada em que a revolução permeia por conta das tecnologias inseridas em um ambiente globalizado e principalmente interconectado, a amplitude e profundidade das mudanças que as mencionadas tecnologias escoam em horizontes jamais

²⁸ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

²⁹ SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1a ed. São Paulo: Edipro, 2016.

³⁰ VAINZOF, Rony. **Relatório de impacto à proteção de dados pessoais**. In: Renato Opice Blum. (Org.). **Proteção de Dados - Desafios e Soluções na Adequação à Lei**. 1ed. Rio de Janeiro: Forense, 2020, v. 1, p. 141-168.

³¹ SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1a ed. São Paulo: Edipro, 2016.

experimentados por parte das revoluções anteriores, alterando a sociedade, economia e neste momento o próprio ser humano em si e, por fim, o impacto sistêmico causados ao nível de Estados soberanos, bem como em sua estrutura interna, tal como órgãos do governo e toda a sociedade em si.

Em virtude disso, é incontestável que os ordenamentos jurídicos democráticos contemporâneos têm progressivamente incorporado mecanismos emergenciais e de caráter mitigatório, no intento de enfrentar as ameaças à segurança dos cidadãos e à proteção de seus dados, sob este aspecto observa-se a nova necessidade de revisão e adaptação de institutos dogmáticos tradicionais, ou até mesmo a criação de novos, com o propósito de atender adequadamente a essas demandas emergentes³².

1.1.1 Evolução Histórica da Tutela Jurisdicional Acerca da Proteção e Privacidade de Dados no Contexto Europeu e Brasileiro

A partir do viés de globalização apresentado, é necessário expor o desenvolvimento histórico perpetrado para que o ordenamento jurídico brasileiro concluísse pela positivação do direito à proteção e à privacidade de dados, fator basilar para consagrar a importância da tomada de providências técnicas e administrativas no contexto de governança digital.

Em um primeiro momento, destaca-se que o ensaio realizado busca evidenciar o contexto histórico dos diplomas legais surgidos, temática alheia ao marco teórico do direito à privacidade suscitado por Brandeis e Louis no artigo “*The Right to Privacy*” publicado em 1930 na revista de Harvard³³.

Por meio deste parâmetro, aponta-se a Convenção Europeia dos Direitos do Homem (CEDH), publicada no ano de 1950 pelo Conselho da Europa, cujo

³² LEAL, Rogério Gesta. **Limites do Direito Fundamental à Proteção de Dados em Face da Instrução Probatória no Processo Penal**. REVISTA NOVOS ESTUDOS JURÍDICOS -ELETRÔNICA, VOL. 28 -N. 1-JAN-ABR2023Disponível em: [periódicosunivali.br](https://doi.org/10.14210/nej.v28n1.p71-93) DOI: <https://doi.org/10.14210/nej.v28n1.p71-93>.

³³ DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thompson Reuters, 2020. 364 p.

surgimento teve início nas cinzas criadas pela Segunda Guerra Mundial pelos Estados dotados de soberania no continente europeu, a fim de possibilitar o estado de direito, a democracia, os direitos humanos e o desenvolvimento social³⁴.

Nessa toada, os Estados participantes do Conselho da Europa (CdE) comprometeram-se, neste plano, com o cumprimento das disposições contidas na CEDH, tal como em recepcionar o diploma nos respectivos ordenamentos jurídicos de cada Estado. Neste sentido, os membros componentes sujeitaram-se à jurisdição do Tribunal Europeu dos Direitos do Homem (TDEH), o qual foi estabelecido no ano de 1959 na cidade de Estrasburgo, França³⁵.

Nesse contexto de relacionamentos apreensivos na seara jurídico-internacional que há o surgimento do direito à proteção de dados pessoais, previsão expressamente contida e tutela por meio do artigo 8º da Convenção Europeia dos Direitos do Homem, nestes termos:

ARTIGO 8º Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.³⁶

A partir da análise do trecho supramencionado, denota-se um marco da proteção e normatização do direito à privacidade de todos os indivíduos, de forma que a mencionada tutela foi assegurada em elemento extensivo à proteção de dados a partir da jurisprudência firmada pelo TEDH, cujo entendimento a época trouxe

³⁴ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 09 de mai. 2024.

³⁵ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 09 de mai. 2024.

³⁶ UNIÃO EUROPEIA. CEDH de 04 de novembro de 1950. **Convenção Europeia dos Direitos do Homem**. Roma, 1950.

inovação ao judiciário ao julgar casos de interceptação comunicacional, diversas formas de vigilância e espionagem, sinalizando, assim, o marco internacional da proteção e privacidade de informações.

Sendo que se baseou nas obrigações contidas no artigo 8º da CEDH, não se limitando à mera proibição da violação à privacidade por parte dos Estados soberanos em si, mas também instituindo na característica de obrigação positiva, no intento de garantir ativamente a tutela da vida privada e familiar³⁷.

Embora houvesse o surgimento da positivação à proteção e privacidade de informações, o período da década de 60 foi grifado pelo desenvolvimento desenfreado de tecnologias, momento em que se ascendeu a necessidade de implementação de normas mais complexas acerca da proteção de dados pessoais, logo, em meio ao período da década de 70, o contexto legislativo europeu foi abrangido pela positivação de diversas resoluções e instruções complementares a respeito da proteção de dados pessoais fundamentadas no artigo 8º da CEDH, as quais tiveram origem o Comitê de Ministros do Conselho da Europa³⁸.

Nesse sentido, os membros responsáveis pela elaboração do Manual da Legislação Europeia sobre a Proteção de Dados abarcam que a Convenção nº 108, diploma que aborda a proteção das pessoas e o tratamento automatizado de dados de caráter pessoal, reverte-se no “único instrumento internacional juridicamente vinculativo no campo da proteção de dados”³⁹.

No que diz respeito à mencionada Convenção nº 108, sua relevância respalda-se em grande notoriedade ao alcance da garantia da privacidade de

³⁷ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 09 de mai. 2024.

³⁸ DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thompson Reuters, 2020. 364 p.

³⁹ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 09 de mai. 2024.

indivíduos, haja vista sua amplitude na regulação das atividades de tratamento realizadas pelos setores públicos e privados⁴⁰.

Sob a perspectiva deste contexto de evolução da proteção e privacidade de dados nos países da União Europeia, ocorre a ascensão dos princípios fundamentais ao tratamento lícito de dados, os quais mandatoriamente teriam de contemplar o preenchimento de finalidade, proporcionalidade e ciclicidade do tempo de vida dos dados, instituídos a partir do impulso gerado pela Convenção 108.

Todavia, cumpre mencionar que o estabelecimento de diplomas normativos que versem acerca da transferência e fluxo internacional de dados a Estados alheios à União Europeia foram instituídos tão somente em 1999, fator que caracteriza uma regulação tardia quando analisada ao lado da necessidade gerada pela matéria.

Ao observar as normas de proteção de dados presentes no contexto jurídico da União Europeia, torna-se difícil eximir-se da Diretiva 95/46/CE, estabelecido por meio do Parlamento Europeu e do Conselho Europeu em 24/10/1985, cuja regulamentação dispôs sobre o tratamento e circulação de dados pessoais.

No plano de implementação Diretiva, variados entes soberanos haviam instituídos legislações nacionais versando sobre a proteção de dados, conseqüentemente a missão da Diretiva foi no sentido de instaurar harmonia entre os ordenamentos internos, no intuito de desembocar em uma livre e despreocupada “circulação de mercadorias capitais, serviços e pessoas no mercado interno”⁴¹, contexto este curiosamente análogo ao surgimento da Lei Geral de Proteção de

⁴⁰ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 09 de mai. 2024.

⁴¹ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 09 de mai. 2024.

Dados⁴² no Brasil, diferindo apenas nos objetivos de regulação entre países membro da União Europeia.

Na temática de direitos humanos na esfera europeia, cita-se a Carta dos Direitos Fundamentais da União Europeia, a qual foi devidamente proclamada em 2000, o mencionado diploma tratou de observar um agrupamento de costumes e obrigações internacionais acordadas entre os Estados-membros, tratando acerca de todos os direitos das esferas cível, política, econômica e social de todos os indivíduos tutelados pelo ordenamento europeu⁴³.

Imperioso expor que, em um primeiro momento, a Carta possuía cunho meramente político, entretanto, com o decorrer do tempo a normativa recebeu elemento juridicamente vinculativo, de forma que expõe e garante o respeito pela vida privada e familiar a partir da previsão contida no artigo 7º, assim como expõe o direito à proteção de dados no artigo seguinte (8º), cenário que eleva a proteção de dados ao grau de direito fundamental tutelado pela União Europeia.

Progredindo-se com o ensaio do cenário legislativo da proteção e privacidade de dados, a CdE, durante o ano de 2012, instituiu uma proposta normativa que possuía o objetivo de preencher as inseguranças causadas pelo contexto social marcado pelo desenvolvimento de tecnologias desenfreadas, haja vista a necessidade de reformar a legislação sobre a matéria. Tal proposta possuía fundamento o desenvolvimento e promulgação de um “Regulamento Geral sobre a Proteção de Dados” e na renovação sobre a Diretiva de Proteção de Dados.

Ante os diversos diplomas legais supramencionados somados aos avanços tecnológicos, a linha histórica de desenvolvimento e positivação do direito à proteção e privacidade de dados é marcada pela regulação europeia sobre proteção de dados, renomada legislação nomeada pelo *General Data Protection Regulation*⁴⁴,

⁴² 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.

⁴³ CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: <http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf> Acesso em: 09 de mai. 2024.

⁴⁴ UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE**

diploma que possui ampla relevância internacional, bem como na cristalina influência causada na geração da Lei Geral de Proteção de Dados.

No que diz respeito ao caso do Brasil, apesar de que a Lei Geral de Proteção de Dados vem à tona apenas no ano de 2018, houve igualmente uma escadaria legislativa permeada para que se alcançasse este patamar. A Constituição Cidadã⁴⁵ foi o primeiro documento jurídico relevante ao ordenamento jurídico brasileiro, o qual evidenciou de forma explícita o direito à vida privada e à intimidade, com fulcro ao art. 5º, inciso X, CF/1988, assim como elegeu a privacidade ao patamar de direito fundamental, causando um grande marco legislativo para a tutela da privacidade na legislação brasileira.

Apesar do mencionado marco legislativo, importante ressaltar que a privacidade era tutelada de forma implícita, isto porque o direito à privacidade remete diversos outros direitos fundamentais (igualdade, da liberdade de escolha, não discriminação, entre outros), logo estava implícito dentro de legislações e matérias esparsas no ordenamento jurídico brasileiro, exemplo disso é a proteção à propriedade dos indivíduos, tema que não deixam de abarcar a privacidade dos mesmos em um segundo plano, distante do texto explícito⁴⁶.

Tal como ocorreu na União Europeia, a sociedade tecnológica formada no início do século 21 foi fundamental para os desdobramentos jurídicos que tornaram possíveis a elaboração de legislações específicas sobre a privacidade e proteção de dados no ordenamento jurídico brasileiro, uma vez que a legislação admite a necessidade de eleger a regulação de espaços e situações específicas diante de um desenvolvimento legislativo⁴⁷ ao mesmo tempo em que tenta alcançar os avanços da tecnologia, exemplo disso é o advento do Marco Civil da Internet, numerada como a

(**Regulamento Geral sobre a Proteção de Dados**). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>>. Acesso em: 26 Set 2023.

⁴⁵ BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 abr. 2023.

⁴⁶ DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 2. ed. São Paulo: Thompson Reuters, 2020. 364 p.

⁴⁷ DAL RI, Luciene. **O Costume Constitucional no Brasil Império: Elemento para a Construção do Estado de Direito?**. História Constitucional (OVIEDO), v. 1, p. 1257-1275, 2024.

Lei 12.965/2014⁴⁸, Lei da qual estampa e exclama em seu preâmbulo que adveio para “estabelecer princípios, garantias, direitos e deveres” para o uso da Internet no Brasil.

Nessa toada, o Senado Federal protocolou a Proposta de Emenda à Constituição n. 17/2019, devidamente aprovada e revertida na Emenda Constitucional 115/2022, a qual prevê o direito à proteção de dados pessoais a título de direito fundamental.

Em vista da recém adição à Constituição, importa-se expor a relevância temática e a necessidade de adotar um programa de governança digital, assim como explorar a direta relação entre governança digital no PJSC o viés garantista de direitos dos titulares previstos no inciso LXXIX, art. 5º da Constituição Federal⁴⁹ e no art. 15º da Lei 13.709/2018⁵⁰.

1.1.2.1. A Importância da Governança Digital em um ordenamento que tutela a proteção e privacidade de dados como direito fundamental

São inúmeros os benefícios obtidos a partir do desenvolvimento de novas tecnologias, no entanto, na mesma medida é possível enumerar suas desvantagens e perigos iminentes, considerando que na mesma medida em que os bancos implementam governança em seus procedimentos, a fim de garantir a segurança e bom funcionamento dos serviços relacionados ao manuseio e guarda de cédulas, igualmente o governo federal necessitou tomar medidas, a fim de resguardar os ambientes tecnológicos e o novo ativo econômico, os dados.

⁴⁸ BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 26 de outubro de 2023.

⁴⁹ BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 5 out. 1988.

⁵⁰ 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 05 mai. de 2023.

Nesse sentido, destaca-se que o governo brasileiro recebeu reconhecimento internacional sobre sua digitalização, sendo inclusive notado pela Organização das Nações Unidas (ONU) após divulgação do Índice de Serviços Online, cujo objetivo é a utilização de tecnologias aplicadas pelo governo no âmbito do fornecimento de serviços públicos, ocupando o 20º lugar dentre 193 Estados analisados⁵¹.

Sob a mesma perspectiva de digitalização do governo, o Brasil obteve o 7º índice mais elevado no *GovTech Maturity Index 2020*⁵², relatório produzido pelo Banco Mundial que contou com a análise de 198 Países, sendo que, segundo o índice do *GovTech Maturity Index 2022*, divulgado em 16/11/2022, o Brasil foi reconhecido como o 2º país de todo o globo com a maior maturidade em governo digital⁵³.

Em vista disso, a governança digital mostra-se um fator indeclinável em razão da necessidade de garantir a proteção de direitos fundamentais e panoramas de segurança nacional, convergente com os ensinamentos de Buz⁵⁴.

Eduardo A. Lamy e Ana C. F. Lamy⁵⁵ destacam a estreita relação entre as temáticas do compliance empresarial no que tange ao estabelecimento de políticas internas e a criação de procedimentos, a fim de garantir o resguardo dos direitos dos titulares de dados, mais especificamente à segurança das informações.

Importante trazer à baila que a partir da década de 1990, o Brasil empreendeu um movimento substancial de reforma do Estado, motivado pela

⁵¹ AEDTNI – Associação de Empresas de Desenvolvimento Tecnológico Nacional e Inovação. **Brasil está entre os 20 países com melhor oferta de serviços públicos digitais.** Disponível em: <https://pedbrasil.org.br/brasil-esta-entre-os-20-paises-com-melhor-oferta-de-servicos-publicos-digitais/>. Acesso em: 09 nov. 2023.

⁵² MINISTÉRIO DA ECONOMIA. **Brasil é reconhecido pelo Banco Mundial como o 7º líder em Governo Digital entre 198 países.** Disponível em: <https://www.gov.br/governodigital/pt-br/noticias/brasil-e-reconhecido-pelo-banco-mundial-como-o-7o-lider-em-governo-digital-entre-198-paises>. Acesso em: 09 de nov. 2023.

⁵³ MINISTÉRIO DA ECONOMIA. **Brasil é reconhecido como segundo líder em governo digital no mundo.** Disponível em: <https://www.gov.br/economia/pt-br/assuntos/noticias/2022/novembro/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo>. Acesso em: 19 de nov. 2023.

⁵⁴ BUZ, Marcelo. A importância da identificação digital segura: confiança. In: BLUM, Renato Opice; WAJSBROT, Shirley (org.). **Cyber Risk Estratégias: estratégias nacionais e corporativas sobre riscos e segurança cibernética.** São Paulo: Thompson Reuters Brasil, 2020. Cap. 3. p. 61-85.

⁵⁵ LAMY, Ana Carolina Faraco; LAMY, Eduardo de Avelar. **Compliance Empresarial.** 1º Edição, Rio de Janeiro: Forense, 2022.

imperiosa necessidade de modernizar a administração pública e enfrentar os desafios inerentes a um contexto marcado por crises fiscais e ineficiências na prestação de serviços públicos. Dentre as medidas implementadas nesse interregno, destacam-se a criação do Ministério da Administração Federal e Reforma do Estado (MARE), a promulgação da Lei de Responsabilidade Fiscal (LRF) e a instituição do Programa Nacional de Desburocratização⁵⁶.

As reformas postas em prática desde então propiciaram avanços significativos na governança pública brasileira. A LRF, por exemplo, desempenhou um papel crucial na estabilização macroeconômica e na promoção da disciplina fiscal, enquanto o Programa Nacional de Desburocratização visou a simplificação dos processos administrativos e a redução da burocracia⁵⁷. Além disso, registraram-se progressos notáveis na esfera da transparência e do acesso à informação, culminando com a aprovação da Lei de Acesso à Informação (LAI) em 2011⁵⁸.

Não obstante os avanços observados, a governança pública brasileira ainda enfrentava desafios consideráveis no período que precedeu o Decreto 9319/2018. A complexidade da máquina pública, a prevalência de uma cultura burocrática, a falta de integração entre os órgãos governamentais, a fragilidade dos mecanismos de controle e a insuficiência de investimentos em tecnologias da informação e comunicação figuravam entre os principais entraves a serem superados⁵⁹.

⁵⁶ JUNIOR, Olavo Brasil de Lima. **As Reformas Administrativas no Brasil: modelos, sucessos e fracassos**. São Paulo: Revista do Serviço Público, 1998.

⁵⁷ TAVARES, André Afonso; BITENCOURT, Caroline Müller. A Lei do Governo Digital e os Laboratórios de Inovação: Inteligência Artificial, Ciência de Dados e Big Open Data como ferramentas de apoio à Auditoria Social e Controle Social. In: MOTTA, Fabrício; VALLE, Vanice Regina Lírio do. (Coords). **Governo Digital e a busca por inovação na Administração Pública**: a Lei n. 14.129, de 29 de março de 2021. Belo Horizonte: Fórum, 2022.

⁵⁸ VALLE, Vivian Cristina Lima López; GALLO, William Ivan. **Inteligência artificial e capacidades regulatórias do Estado no ambiente da administração pública digital**. A&C – Revista de Direito Administrativo e Constitucional. Belo Horizonte, ano 20, n. 82, pp. 67- 86, out./dez. 2020. Disponível em: https://www.academia.edu/47798775/Intelig%C3%A2ncia_artificial_e_capacidades_regul%C3%B3rias_do_Estado_no_ambiente_da_administra%C3%A7%C3%A3o_p%C3%BAblica_digital. Acesso em: 24 jul. 2024.

⁵⁹ VIANNA, Bernardo. **Digitalização do setor público é crucial para o desenvolvimento sustentável**. Notícias. Insper. 13/04/2022. Disponível em: <https://www.insper.edu.br/noticias/digitalizacao-do-setor-publico-e-crucial-para-odesenvolvimentosustentavel/#:~:text=O%20%C3%8Dndice%20de%20Desenvolvimento%20em,servi%C3%A7os%20p%C3%BAblicos%20por%20meios%20digitais>. Acesso em: 22 set. 2024.

Uma análise do cenário anterior ao Decreto 9319/2018 revela um sistema de governança com características que limitavam a eficiência e eficácia da administração pública. A centralização decisória concentrava as decisões de maior relevância em poucos níveis hierárquicos, restringindo a autonomia e a agilidade da gestão pública. A cultura burocrática prevalecente e a existência de processos administrativos intrincados e morosos comprometiam o funcionamento do setor público⁶⁰. A ausência de mecanismos de controle eficientes dificultava a prevenção e o combate à corrupção, ao desperdício e à malversação de recursos públicos⁶¹. A participação da sociedade civil na formulação e no monitoramento das políticas públicas era limitada, prejudicando a legitimidade e a eficácia da gestão pública⁶².

Adicionalmente, a carência de uma cultura de gestão de riscos aumentava a vulnerabilidade da administração pública a eventos adversos que poderiam comprometer o alcance dos objetivos estratégicos⁶³. Finalmente, a insuficiência de investimentos em tecnologias da informação e comunicação obstaculizava a modernização da gestão pública e a oferta de serviços públicos digitais eficientes⁶⁴.

Em resumo, a modernização da administração pública brasileira, iniciada na década de 1990, trouxe avanços significativos. Contudo, os desafios remanescentes exigiram uma abordagem contínua e integrada para alcançar níveis

⁶⁰ VALLE, Vivian Cristina Lima López; GALLO, William Ivan. **Inteligência artificial e capacidades regulatórias do Estado no ambiente da administração pública digital**. A&C – Revista de Direito Administrativo e Constitucional. Belo Horizonte, ano 20, n. 82, pp. 67- 86, out./dez. 2020. Disponível em: https://www.academia.edu/47798775/Intelig%C3%A2ncia_artificial_e_capacidades_regul%C3%B3rias_do_Estado_no_ambiente_da_administra%C3%A7%C3%A3o_p%C3%BAblica_digital. Acesso em: 24 jul. 2024.

⁶¹ SECHI, Leonardo. **Análise de políticas públicas: diagnósticos de problemas, recomendações de soluções**. São Paulo: Cengage Learning, 2019.

⁶² SECHI, Leonardo. **Análise de políticas públicas: diagnósticos de problemas, recomendações de soluções**. São Paulo: Cengage Learning, 2019.

⁶³ TAVARES, André Afonso; BITENCOURT, Caroline Müller. A Lei do Governo Digital e os Laboratórios de Inovação: Inteligência Artificial, Ciência de Dados e Big Open Data como ferramentas de apoio à Auditoria Social e Controle Social. In: MOTTA, Fabrício; VALLE, Vanice Regina Lírio do. (Coords). **Governo Digital e a busca por inovação na Administração Pública**: a Lei n. 14.129, de 29 de março de 2021. Belo Horizonte: Fórum, 2022.

⁶⁴ VIANNA, Bernardo. **Digitalização do setor público é crucial para o desenvolvimento sustentável**. Notícias. Insper. 13/04/2022. Disponível em: <https://www.insper.edu.br/noticias/digitalizacao-do-setor-publico-e-crucial-para-o-desenvolvimento-sustentavel/#:~:text=O%20C3%8Dndice%20de%20Desenvolvimento%20em,servi%C3%A7os%20p%C3%BAblicos%20por%20meios%20digitais>. Acesso em: 22 set. 2024.

mais elevados de eficiência, transparência e participação social na governança pública⁶⁵.

1.1.2.2. Conceituando “governança digital” sob o viés da administração pública

Tendo em vista a natureza dinâmica envolto do termo "governança digital", não se torna o propósito desta dissertação a propositura de uma definição estática. O real objetivo é expor as diferentes interpretações presentes na literatura, a fim de fornecer uma definição operacional.

Segundo Danusa Gomes, “a governança digital apresenta-se como um novo modelo de gestão que “se aproxima mais do modelo gerencial com características do modelo societal de administração pública”⁶⁶. A governança, sob custódia da tecnologia é “uma resposta ao aumento da complexidade da sociedade em relação à globalização e à evolução dos meios de comunicação”, sendo considerada uma “tendência emergente para reinventar o funcionamento do governo”⁶⁷.

Na mesma senda, Tiago José de Souza Lima Bezerra expõe que, com a introdução das Tecnologias da Informação e Comunicação (TIC) na dinâmica dos

⁶⁵ NOHARA, Irene. Desafios de Inovação na Administração Pública contemporânea: “destruição criadora” ou “inovação destruidora” do Direito Administrativo? **Direito Administrativo**. 22/04/2020. Disponível em: <https://direitoadm.com.br/desafios-de-inovacaona-administracao-publica-contemporanea-destruicao-criadora-ou-inovacao-destruidora-dodireito-administrativo/>. Acesso em: 20 set. 2024.

⁶⁶ GOMES, Danusa Fernandes Rufino. **Governança Digital: desenvolvimento de um índice para autarquias públicas federais vinculadas ao Ministério da Educação**. 162 fls. 2018. Dissertação (Mestrado em Administração Pública). Programa de Pós-graduação em Administração Pública da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da Universidade de Brasília. Brasília, 2018, p. 56. Disponível em: <https://repositorio.unb.br/handle/10482/32724>. Acesso em: 06 out. 2024.

⁶⁷ GOMES, Danusa Fernandes Rufino. **Governança Digital: desenvolvimento de um índice para autarquias públicas federais vinculadas ao Ministério da Educação**. 162 fls. 2018. Dissertação (Mestrado em Administração Pública). Programa de Pós-graduação em Administração Pública da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da Universidade de Brasília. Brasília, 2018, p. 56. Disponível em: <https://repositorio.unb.br/handle/10482/32724>. Acesso em: 06 out. 2024.

processos e atividades públicas, torna-se necessária a revisão e adequação tanto dos processos internos quanto da estrutura organizacional⁶⁸.

Tal entendimento encontra respaldo no disposto pelo Decreto nº 9.203/2017, que, em seu art. 2º, I, define a governança pública como um conjunto de mecanismos de liderança, estratégia e controle implementados para avaliar, direcionar e monitorar a gestão, com o objetivo de conduzir políticas públicas e prestar serviços de interesse da sociedade⁶⁹.

Da mesma forma, a Instrução Normativa Conjunta MP/CGU nº 01/2016, em seu art. 2º, VIII e IX, conceitua a governança como uma combinação de processos e estruturas estabelecidas pela alta administração, com a finalidade de informar, direcionar, administrar e monitorar as atividades da organização, visando alcançar seus objetivos, sobretudo na condução de políticas públicas e na prestação de serviços de interesse público⁷⁰.

Por sua vez, Francis Idzi compreende a governança na era digital como parte de uma nova fase da Nova Gestão Pública. Esse movimento envolve a "adoção de estruturas holísticas que respondem às necessidades de digitalização gradual dos processos burocráticos", o que acarreta uma "ampla gama de mudanças cognitivas, comportamentais, organizacionais, políticas e culturais associadas aos sistemas de informação"⁷¹.

⁶⁸ BEZERRA, Tiago José de Souza Lima. **A constitucionalização da democracia digital no direito brasileiro: a regulação das políticas e estratégias de governança digital na Administração Pública Federal**. 192 fls. 2020. Dissertação (Mestrado em Direito). Programa de Pós-graduação em Direito da Universidade Federal do Rio Grande do Norte. Natal, 2020, p. 137. Disponível em: <https://repositorio.ufrn.br/handle/123456789/31720>. Acesso em: 06 out. 2024.

⁶⁹ BRASIL. **Decreto nº. 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em: 06 out. 2024.

⁷⁰ BRASIL. Instrução Normativa Conjunta nº. 1, de 10 de maio de 2016. **Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal**. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em: 06 jan. 2023.

⁷¹ IDZI, Francis Michael. **Governança digital: análise de componentes chave, modelos de contratos sociais e barreiras para o design de políticas públicas**. 100 fls. 2021. Dissertação (Mestrado em Políticas Públicas). Escola de Políticas Públicas e Governo da Fundação Getúlio Vargas. Brasília, 2021, p. 24. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31436>. Acesso em: 14 out. 2024.

Nesse contexto, a governança digital constitui um paradigma da Administração Pública em desenvolvimento, conceito ainda não consolidado e objeto de debate no meio acadêmico⁷².

Contudo, no intuito de estabelecer parâmetros acadêmicos sob a análise da presente dissertação, adota-se o conceito trazido por Ariê Scherreier Ferneda, qual seja:

“uma forma de estabelecer o alinhamento estratégico da organização pública ao uso/gestão das TIC. Para isso, deve-se considerá-las como aliadas capazes de auxiliar a tomada de decisão com a finalidade de ampliar a participação social e cidadã por meio da transparência e com vistas a orientar a organização à satisfação das demandas internas e externas de forma responsiva e célere.” (p. 77)⁷³

Isto porque Ferneda extrai o referido conceito a partir do equilíbrio de diversos eixos da governança digital, sendo a) a função da governança digital; b) a governança como alinhamento estratégico e apoio da tomada de decisão; e c) governança digital aplicada ao setor público como um modelo de gestão.

1.1.2.3. Contornos Jurídicos: Situando a governança digital no ordenamento jurídico brasileiro

Muito embora o termo governança seja amplamente abarcado no mundo corporativo privado, a relevância da matéria toma espaço mediante os entes públicos

⁷² IDZI, Francis Michael. **Governança digital: análise de componentes chave, modelos de contratos sociais e barreiras para o design de políticas públicas**. 100 fls. 2021. Dissertação (Mestrado em Políticas Públicas). Escola de Políticas Públicas e Governo da Fundação Getúlio Vargas. Brasília, 2021, p. 24. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31436>. Acesso em: 14 out. 2024.

⁷³ FERNE+DA, Ariê Scherreier. **Governança e transformação digital nas capitais dos estados brasileiros: as Tecnologias da Informação e Comunicação como aliadas estratégicas da Administração Pública Municipal**. 225 fls. 2023. Dissertação (Mestrado em Direito). Universidade Federal de Santa Catarina. Florianópolis, 2023.

por meio do estabelecimento de Resoluções, Decretos, Leis e entre outros dispositivos vinculativos na seara pública.

Por essa razão, é necessária uma exposição acerca dos atos que traduzem a postura e a estratégia dos entes públicos frente às inseguranças trazidas em meio à utilização de tecnologias e lacunas jurídicas criadas pelas mesmas, de modo a elucidar com maior precisão as melhores práticas de governança, inclusive as que são atualmente praticadas pelos entes.

1.1.2.4. O Decreto 9.319/2018 - Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital.

A temática recebeu relevância após edição do Decreto 9.319/2018⁷⁴ que implementou uma estrutura de governança no que diz respeito à implementação da Estratégia Brasileira para a Transformação Digital, a qual prevê a confiança no ambiente digital como um de seus pilares, haja vista que o desenvolvimento da economia digital necessita da confiança no mencionado ambiente, dito isso, é mandatório que a ação governamental esteja focada na (i) proteção de direitos e privacidade e (ii) defesa e segurança do ambiente digital.

Sendo assim, o Decreto 9319/2018, promulgado em 29 de outubro de 2018, representa um marco significativo na trajetória em direção a uma administração pública mais eficiente e alinhada com as melhores práticas de governança.

A elaboração deste Decreto ocorreu em um contexto de demandas crescentes por maior eficiência, transparência e accountability na gestão pública, motivadas por vários fatores convergentes. A crise econômica e fiscal vigente impôs a necessidade imperativa de otimizar os recursos públicos e maximizar os resultados em um cenário de severa restrição financeira⁷⁵. Além disso, a sucessão de escândalos

⁷⁴ BRASIL. **Decreto nº 9.319, de 21 de março de 2018.** Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.html. Acesso em: 15 mai. 2022.

⁷⁵ PIRES, Tatieures Gomes. **Uma avaliação da implantação da Política de Governança Digital na Universidade Federal do Ceará.** 208 fls. 2019. Dissertação (Mestrado Profissional). Programa de Pós-graduação Profissional em Avaliação de Políticas Públicas da Universidade Federal do Ceará.

de corrupção que assolou o país nas últimas décadas comprometeu a credibilidade da gestão pública, evidenciando a necessidade urgente de fortalecer os mecanismos de controle e promover a integridade administrativa⁷⁶. Outro fator relevante foi a influência de organismos internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que têm exercido uma crescente pressão sobre a agenda de reformas na governança pública globalmente, impactando também o Brasil⁷⁷. Paralelamente, a população brasileira mostrou-se cada vez mais exigente em relação à qualidade dos serviços públicos, pressionando a administração pública a encontrar soluções inovadoras e eficientes para atender às suas demandas crescentes⁷⁸.

O Decreto 9319/2018 tem como objetivo central "estabelecer diretrizes para a governança e a gestão de riscos no âmbito dos órgãos e das entidades da administração pública federal, visando ao alcance de resultados para a sociedade, ao aumento da accountability, à melhoria da gestão dos recursos públicos, ao fortalecimento da prevenção e do combate à corrupção e ao incremento da capacidade de entregar serviços de qualidade ao cidadão"⁷⁹. Em síntese, o Decreto ambiciona fomentar uma mudança cultural na administração pública, promovendo

Fortaleza, 2019, p. 79. Disponível em: https://repositorio.ufc.br/bitstream/riufc/49953/3/2019_dis_tgpires.pdf. Acesso em: 13 out. 2024.

⁷⁶ RODRIGUES, Mariane Pires. **Governança Digital e transparência pública: uma análise das prefeituras paranaenses**. 183 fls. 2016. Dissertação (Mestrado em Ciência Política). Programa de Pós-Graduação em Ciência Política, Setor de Ciências Humanas, Letras e Artes, Universidade Federal do Paraná. Curitiba, 2016. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/45907/R%20-%20D%20-%20MIRIANE%20PIRES%20RODRIGUES.pdf?sequence=1&isAllowed=y>. Acesso em: 06 out. 2024.

⁷⁷ OCDE. **Government at a Glance: Latin America and the Caribbean 2017**. Paris: OECD Publishing, 2016.

⁷⁸ RODRIGUES, Mariane Pires. **Governança Digital e transparência pública: uma análise das prefeituras paranaenses**. 183 fls. 2016. Dissertação (Mestrado em Ciência Política). Programa de Pós-Graduação em Ciência Política, Setor de Ciências Humanas, Letras e Artes, Universidade Federal do Paraná. Curitiba, 2016. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/45907/R%20-%20D%20-%20MIRIANE%20PIRES%20RODRIGUES.pdf?sequence=1&isAllowed=y>. Acesso em: 06 out. 2024.

⁷⁹ BRASIL. **Decreto 9319, de 29 de outubro de 2018**. Estabelece diretrizes para a governança e gestão de riscos no âmbito dos órgãos e entidades da administração pública federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 2018.

uma gestão orientada para resultados, focada na geração de valor público e na satisfação das necessidades sociais⁸⁰.

Para alcançar seus objetivos, o Decreto 9319/2018 introduz uma série de inovações significativas na governança pública brasileira. Uma destas inovações é a formalização da governança, estabelecendo diretrizes e princípios claros pela primeira vez, delineando papéis, responsabilidades e mecanismos de funcionamento dentro da administração pública federal⁸¹. A gestão de riscos é outra inovação crucial, exigindo que todos os órgãos e entidades implementem uma gestão de riscos de forma integrada, com o intuito de antecipar e mitigar eventos adversos que possam comprometer os objetivos estratégicos⁸².

O Decreto também reforça o papel do controle interno, atribuindo-lhe a responsabilidade contínua de avaliação e monitoramento da governança e da gestão de riscos, crucial para assegurar a eficácia das práticas implementadas⁸³. Adicionalmente, o Decreto enfatiza a transparência e a participação social na gestão pública, estabelecendo mecanismos destinados a ampliar o acesso à informação e a incentivar o controle social⁸⁴. Por último, reconhece a importância das tecnologias da informação e comunicação para a modernização da gestão pública, promovendo seu

⁸⁰ PIRES, Tatieuress Gomes. **Uma avaliação da implantação da Política de Governança Digital na Universidade Federal do Ceará**. 208 fls. 2019. Dissertação (Mestrado Profissional). Programa de Pós-graduação Profissional em Avaliação de Políticas Públicas da Universidade Federal do Ceará. Fortaleza, 2019, p. 79. Disponível em: https://repositorio.ufc.br/bitstream/riufc/49953/3/2019_dis_tgpires.pdf. Acesso em: 13 out. 2024.

⁸¹ SANTOS, Matheus Henrique de Souza. **Aspectos da governança digital na administração pública federal do Brasil sob a luz das orientações da OCDE**. Revista Tempo do Mundo, n. 25, 331-355, abr. 2021. Disponível em: <https://www.ipea.gov.br/revistas/index.php/rtm/article/view/279>. Acesso em: 20 out. 2024.

⁸² SANTOS, Matheus Henrique de Souza. **Aspectos da governança digital na administração pública federal do Brasil sob a luz das orientações da OCDE**. Revista Tempo do Mundo, n. 25, 331-355, abr. 2021. Disponível em: <https://www.ipea.gov.br/revistas/index.php/rtm/article/view/279>. Acesso em: 20 out. 2024.

⁸³ SANTOS, Roberval de Jesus Leone dos. **Rede Governo: o Portal de Serviços e Informações para o Cidadão**. Relato de experiência. Iniciativa premiada no 7º Concurso Inovação na Gestão Pública Federal. Prêmio Hélio Beltrão – 2002. Disponível em: https://repositorio.enap.gov.br/bitstream/1/554/1/050_02.pdf. Acesso em: 19 out. 2024.

⁸⁴ SANTOS, Roberval de Jesus Leone dos. **Rede Governo: o Portal de Serviços e Informações para o Cidadão**. Relato de experiência. Iniciativa premiada no 7º Concurso Inovação na Gestão Pública Federal. Prêmio Hélio Beltrão – 2002. Disponível em: https://repositorio.enap.gov.br/bitstream/1/554/1/050_02.pdf. Acesso em: 19 out. 2024.

uso na automatização de processos, na gestão de dados e na oferta de serviços públicos digitais⁸⁵.

O Decreto 9319/2018 representa, assim, um avanço significativo na história da governança pública brasileira. Suas diretrizes e princípios possuem o potencial de transformar a cultura administrativa, promovendo uma gestão mais eficiente, transparente, ética e orientada para a geração de valor público⁸⁶. No entanto, é fundamental reconhecer que a mera promulgação de um decreto não garante sua efetividade. A implementação do Decreto 9319/2018 requer um esforço articulado de gestores públicos, servidores, órgãos de controle e da sociedade em geral, visando assegurar que seus objetivos sejam plenamente atingidos e seus benefícios se revertam em melhorias concretas na vida dos cidadãos⁸⁷.

1.1.2.5. Decreto 10.322/2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

O ordenamento não cessou sua evolução na matéria e instituiu a estratégia de governo digital (2020 a 2022) por meio do Decreto 10.332/2020⁸⁸ cujo

⁸⁵ RODRIGUES, Mariane Pires. **Governança Digital e transparência pública: uma análise das prefeituras paranaenses**. 183 fls. 2016. Dissertação (Mestrado em Ciência Política). Programa de Pós-Graduação em Ciência Política, Setor de Ciências Humanas, Letras e Artes, Universidade Federal do Paraná. Curitiba, 2016. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/45907/R%20-%20D%20-%20MIRIANE%20PIRES%20RODRIGUES.pdf?sequence=1&isAllowed=y>. Acesso em: 06 out. 2024.

⁸⁶ PIRES, Tatieuress Gomes. **Uma avaliação da implantação da Política de Governança Digital na Universidade Federal do Ceará**. 208 fls. 2019. Dissertação (Mestrado Profissional). Programa de Pós-graduação Profissional em Avaliação de Políticas Públicas da Universidade Federal do Ceará. Fortaleza, 2019, p. 79. Disponível em: https://repositorio.ufc.br/bitstream/riufc/49953/3/2019_dis_tgpires.pdf. Acesso em: 13 out. 2024.

⁸⁷ SANTOS, Roberval de Jesus Leone dos. **Rede Governo: o Portal de Serviços e Informações para o Cidadão**. Relato de experiência. Iniciativa premiada no 7º Concurso Inovação na Gestão Pública Federal. Prêmio Hélio Beltrão — 2002. Disponível em: https://repositorio.enap.gov.br/bitstream/1/554/1/050_02.pdf. Acesso em: 19 out. 2024.

⁸⁸ BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília, DF: Presidência da República, 2020. Disponível em: <https://www.in.gov.br/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358>. Acesso em: 05 mai. 2022.

objetivo final é reconquistar a confiança dos brasileiros, uma nobre e urgente medida em respaldo de um cenário virtual inseguro marcado por diversos ataques cibernéticos, motivo pelo qual enseja a grande relevância do presente estudo e demonstra o extenso caminho que os órgãos públicos tem a percorrer para demonstrar a efetiva garantia dos direitos fundamentais à proteção e privacidade de dados.

O Decreto nº 10.332, de 2020, surgiu como uma resposta articulada às condições adversas enfrentadas pelo setor público, demandando uma reformulação estrutural e estratégias concretas para a efetivação da Estratégia de Governo Digital (EGD). A promulgação deste decreto representa um compromisso inabalável do governo brasileiro com a inovação e a transformação digital na esfera pública⁸⁹.

O Decreto nº 10.332, de 2020, estabelece uma série de diretrizes essenciais para a transformação digital no âmbito governamental. Entre essas diretrizes, destaca-se a promoção da interoperabilidade e integração entre diferentes sistemas de informação governamentais. Esse esforço visa à unificação dos serviços digitais em plataformas coesas e integradas, o que é vital para a eficiência administrativa⁹⁰.

Desde sua implementação, tem gerado impactos consideráveis, tanto econômicos quanto sociais. A digitalização de processos administrativos e a interoperabilidade dos sistemas governamentais resultaram em uma melhora significativa na eficiência operacional do setor público. Relatórios da Secretaria de Governo Digital indicam uma notável redução nos prazos de atendimento e nos custos operacionais⁹¹.

⁸⁹ BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022 e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 29 abr. 2020.

⁹⁰ BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022 e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 29 abr. 2020.

⁹¹ SECRETARIA DE GOVERNO DIGITAL. **Relatório de Resultados 2021**. Brasília: Ministério da Economia, 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/secretaria-de-governo-digital>. Acesso em: 21 maio 2024.

A transparência e o controle social também foram beneficiados. A disponibilização de serviços e dados em plataformas digitais facilitou o acesso público à informação governamental, promovendo maior transparência e possibilitando um controle social mais efetivo⁹².

O Decreto nº 10.332, de 28 de abril de 2020, marca um ponto crucial na trajetória de modernização administrativa e transformação digital do governo brasileiro. As diretrizes estabelecidas têm potencial para não apenas melhorar a eficiência e transparência dos serviços públicos, mas também para promover a inclusão digital e intensificar a participação cidadã. No entanto, alcançar plenamente esses objetivos requer superar os desafios persistentes e garantir uma implementação contínua e sustentável das políticas delineadas na EGD.

1.1.2.6. Decreto 10.222/2020 – Estratégia Nacional de Segurança Cibernética

As ameaças cibernéticas no Brasil se manifestam em diversas formas, desde ataques individuais com fins de lucro, como roubo de dados bancários e sequestro de dados (ransomware), até operações sofisticadas de espionagem, sabotagem e disseminação de desinformação, com potencial para causar interrupção em serviços essenciais e comprometer a segurança nacional.

Diante desse cenário desafiador, a segurança cibernética se torna uma questão de Estado, demandando ações coordenadas e eficazes para proteger os interesses nacionais no ambiente digital. É nesse contexto que se insere a Estratégia Nacional de Segurança Cibernética (ENSC), estabelecida pelo Decreto nº 10.222/2020.

O Decreto nº 10.222, de 5 de fevereiro de 2020, marca um divisor de águas na regulamentação da segurança cibernética no Brasil. Sua promulgação não ocorreu de maneira fortuita, mas é fruto de um amadurecimento institucional e de uma

⁹² SECRETARIA DE GOVERNO DIGITAL. **Relatório de Resultados 2021**. Brasília: Ministério da Economia, 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/secretaria-de-governo-digital>. Acesso em: 21 maio 2024.

crescente conscientização sobre a relevância estratégica da proteção do ciberespaço nacional. Este marco legislativo destaca-se como uma resposta coordenada às vulnerabilidades e às ameaças emergentes no ambiente digital⁹³.

A emergência de uma Estratégia Nacional de Segurança Cibernética (ENSC) deu-se pela confluência de múltiplos fatores cruciais. Primeiramente, o aumento da dependência digital foi um aspecto preponderante: a progressiva digitalização da sociedade brasileira, abrangendo desde serviços bancários e transações comerciais até infraestruturas críticas como energia, saúde e transportes, revelou a premente necessidade de mecanismos robustos de defesa contra ameaças cibernéticas⁹⁴. Adicionalmente, o panorama internacional da segurança cibernética tornou-se acentuadamente complexo e desafiante, com o surgimento de novas modalidades de ataque, a atuação de grupos criminosos organizados e a crescente participação de Estados-nação em atividades maliciosas no ciberespaço⁹⁵.

Outro fator relevante foi a participação ativa do Brasil em fóruns internacionais, como a União Internacional de Telecomunicações (UIT) e a Organização dos Estados Americanos (OEA), o que evidenciou a necessidade de alinhar as políticas nacionais de segurança cibernética às melhores práticas e acordos internacionais (GONÇALVES, 2020). Além disso, experiências prévias e lições aprendidas decorrentes de incidentes, como ataques a órgãos governamentais e vazamento de dados sensíveis, sublinharam a importância de aprimorar a capacidade nacional para a prevenção, detecção e resposta a incidentes cibernéticos⁹⁶.

A Estratégia Nacional de Segurança Cibernética, conforme definida pelo Decreto nº 10.222/2020, tem como objetivo primordial "proteger os interesses nacionais no ciberespaço, visando garantir a soberania, os direitos e as liberdades

⁹³ BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Institui a Estratégia Nacional de Segurança Cibernética (ENSC). Diário Oficial da União, Brasília, 5 fev. 2020.

⁹⁴ COBIT 2019 Framework. **Governance and Management Objectives**. ISACA. 2019.

⁹⁵ CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo Digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil**. Sequência. Florianópolis, n. 84, pp. 209-242, abr. 2020, p. 212. Disponível em: <https://www.scielo.br/j/seq/a/f9mk84ktBCQJFzc87BnYgZv/?format=pdf&lang=pt>. Acesso em: 20 out. 2024.

⁹⁶ ROSA, Gabriela. **Prevenção e resposta a incidentes cibernéticos**. Florianópolis: Ed. UFSC, 2020.

dos cidadãos, o desenvolvimento e a defesa nacionais"⁹⁷. Para alcançar esse objetivo macro, a ENSC delineia um conjunto de metas específicas, que incluem a proteção das infraestruturas críticas nacionais contra ataques cibernéticos. Além disso, busca promover a resiliência do ciberespaço, assegurando a continuidade dos serviços essenciais em face de incidentes⁹⁸. Outro aspecto fundamental é o fortalecimento da capacidade nacional de prevenção, detecção e resposta a incidentes cibernéticos, bem como o fomento à cooperação entre setores públicos, privados e a sociedade civil em prol da segurança cibernética⁹⁹. Em paralelo, a ENSC visa desenvolver uma cultura de segurança cibernética abrangente na sociedade brasileira e incentivar a pesquisa, o desenvolvimento e a inovação em tecnologias de segurança cibernética¹⁰⁰.

A estrutura da ENSC está organizada em torno de quatro eixos estratégicos que orientam as ações e iniciativas destinadas ao cumprimento dos objetivos estabelecidos. O primeiro eixo, as ações preventivas, foca na redução da probabilidade de incidentes cibernéticos por meio da implementação de medidas de segurança, sensibilização da sociedade e promoção de boas práticas em segurança cibernética¹⁰¹. O segundo eixo, as ações de defesa, concentra-se na detecção, análise e resposta a incidentes cibernéticos, com vistas a minimizar os impactos decorrentes de ataques e assegurar a continuidade dos serviços essenciais¹⁰². O terceiro eixo, as ações de recuperação, visa restabelecer a normalidade dos serviços e sistemas

⁹⁷ BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. **Institui a Estratégia Nacional de Segurança Cibernética (ENSC)**. Diário Oficial da União, Brasília, 5 fev. 2020.

⁹⁸ CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo Digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil**. Sequência. Florianópolis, n. 84, pp. 209-242, abr. 2020, p. 212. Disponível em: <https://www.scielo.br/j/seq/a/f9mk84ktBCQJFzc87BnYgZv/?format=pdf&lang=pt>. Acesso em: 20 out. 2024.

⁹⁹ FERNANDES, Aguinaldo Aragon. A Governança Digital 4.0. In: FERNANDES, Aguinaldo Aragon; DINIZ, José Luís; ABREU, Vladimir Ferraz de. (Coords.). **Governança Digital 4.0**. Rio de Janeiro: Brasport, pp. 160-205, 2019, p. 202.

¹⁰⁰ FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços**. 2. ed. Rio de Janeiro: Brasport, 2008.

¹⁰¹ FERNANDES, Aguinaldo Aragon; BRITO, Ronaldo; SOUZA, Daniela Emiliano de. **Planejando a Transformação Digital 4.0**. In: FERNANDES, Aguinaldo Aragon; DINIZ, José Luís; ABREU, Vladimir Ferraz de. (Coords.). **Governança Digital 4.0**. Rio de Janeiro: Brasport, pp. 206-220, 2019.

¹⁰² FERNANDES, Aguinaldo Aragon. A Governança Digital 4.0. In: FERNANDES, Aguinaldo Aragon; DINIZ, José Luís; ABREU, Vladimir Ferraz de. (Coords.). **Governança Digital 4.0**. Rio de Janeiro: Brasport, pp. 160-205, 2019, p. 202.

afetados por incidentes cibernéticos, reduzindo prejuízos e fortalecendo a resiliência do ciberespaço brasileiro¹⁰³. Por fim, as ações de fortalecimento envolvem iniciativas para o desenvolvimento da base tecnológica e industrial do país em segurança cibernética, formação de recursos humanos qualificados e o fortalecimento da governança da segurança cibernética no Brasil¹⁰⁴.

A promulgação do Decreto nº 10.222/2020 e a instituição da ENSC constituem um avanço substancial para a consolidação de uma postura estratégica e integrada em relação à segurança cibernética no Brasil. Contudo, a eficácia da Estratégia não se esgota na sua existência normativa; é imperativo que a ENSC seja implementada em ações tangíveis, requerendo o envolvimento ativo de todos os atores pertinentes — governo, setor privado, academia e sociedade civil. A materialização deste marco regulatório em práticas efetivas será determinante para assegurar a proteção do ciberespaço nacional e garantir os interesses estratégicos brasileiros em um mundo cada vez mais digitalizado e interconectado¹⁰⁵.

1.1.2.7. Desafios da Governança Digital – Comitês Gestores

Sob outra perspectiva, o sistema de governança evidencia a existência de embates em sua eficácia, de forma que o mero estabelecimento de políticas ou regimentos orientativos não se revertem no principal motivo para o desenvolvimento de um programa maduro do qual possa prover a tutela dos direitos dos titulares, todavia, o cerne da questão está na forma em que o PJSC oportuna a transmissão de

¹⁰³ FERNEDA, Ariê Scherreier; CRISTÓVAM, José Sérgio da Silva. **Metodologias ágeis para a transformação digital no Brasil: uma análise do Scrum aplicado ao Setor Público**. Direitos Democráticos & Estado Moderno – Revista da Faculdade de Direito da PUC-SP. São Paulo, v. 3, n. 6, pp. 84-101, set./dez. 2022. Disponível em: <https://revistas.pucsp.br/DDEM/article/view/58498>. Acesso em: 19 out. 2024.

¹⁰⁴ CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo Digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil**. Sequência. Florianópolis, n. 84, pp. 209-242, abr. 2020, p. 212. Disponível em: <https://www.scielo.br/j/seq/a/f9mk84ktBCQJFzc87BnYgZv/?format=pdf&lang=pt>. Acesso em: 20 out. 2024.

¹⁰⁵ CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo Digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil**. Sequência. Florianópolis, n. 84, pp. 209-242, abr. 2020, p. 212. Disponível em: <https://www.scielo.br/j/seq/a/f9mk84ktBCQJFzc87BnYgZv/?format=pdf&lang=pt>. Acesso em: 20 out. 2024.

seus valores aos seus *stakeholders*, incluindo-se os co-controladores e suboperadores de dados envolvidos nas atividades de tratamento, como trabalha Ana e Eduardo Lamy¹⁰⁶.

Nesse sentido, ressalta-se o estabelecimento do Comitê Gestor da Internet no Brasil (CGI.br), Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (CGI-ICP Brasil), Comitê Interministerial para a Transformação Digital (CITDigital) e o Comitê Gestor da Identificação Civil Nacional (ICN) por parte do governo brasileiro na tomada de boas práticas de governança digital, fator em que o Poder Judiciário Brasileiro e o PJSC não negligenciam.

Na mesma medida e de forma simétrica, o Conselho Nacional de Justiça (CNJ) implementou a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), a partir da Resolução nº 211/2015¹⁰⁷, a fim de guiar os órgãos do judiciário no que diz respeito à adoção de boas práticas de Governança de Tecnologia da Informação (GTI) e prover o uso da tecnologia de forma aperfeiçoada ao mesmo tempo em que são tomadas ações de melhoria da gestão, infraestrutura de tecnologia da informação e governança.

Em plena sintonia com a estratégia do CNJ e governo federal, o PJSC instituiu o Comitê de Governança de Tecnologia da Informação (CGOVTI) e o Comitê de Gestão de Tecnologia da Informação (CGESTI), a partir da publicação da Resolução nº 31/2018¹⁰⁸, assim como o Comitê de em que pese a mencionada Resolução não tenha previsto explicitamente o objetivo de reconquistar a confiança dos cidadãos e garantir uma efetiva tutela da proteção e privacidade de dados dos titulares, o texto atual foi modificado pela Resolução nº 17/2021¹⁰⁹, a qual respaldou que o Comitê de Governança de Segurança da Informação e o Núcleo de Inteligência

¹⁰⁶ LAMY, Ana Carolina Faraco; LAMY, Eduardo de Avelar. **Compliance Empresarial**. São Paulo: Editora Gen. 2022.

¹⁰⁷ CNJ – Conselho Nacional de Justiça. **Resolução n.º 211, de 15 de dezembro de 2015a**. Disponível em: <<http://www.cnj.jus.br/busca-atos-adm?documento=3052>>. Acesso em: 15 mai. 2024.

¹⁰⁸ TJSC – Tribunal de Justiça de Santa Catarina. **Resolução nº 31/2018**. Disponível em: <http://busca.tjsc.jus.br/buscatextual/integra.do?cdSistema=1&cdDocumento=176659&cdCategoria=1&q=&frase=&excluir=&qualquer=&prox1=&prox2=&prox3=>. Acesso em: 16 mai. 2024.

¹⁰⁹ TJSC – Tribunal de Justiça de Santa Catarina. **Resolução nº 17/2021**. Disponível em: <https://www.tjsc.jus.br/documents/37870/5647413/Resoluc%CC%A7a%CC%83o+Conjunta+GP-CGJ+n.+17-2021.pdf/12c07e35-554e-5512-17e0-3c5967db6458?t=1624485198145> . Acesso em: 16 mai. 2024.

e Segurança Institucional serão responsáveis por garantir a segurança e proteção dos dados pessoais.

Embora reste evidente que os órgãos do judiciário estejam se adequando aos novos cenários tecnológicos, torna-se necessário verificar a efetividade das mencionadas medidas, assim como avaliar o programa de Governança Digital como um todo, a fim de prover uma análise fundamentada em riscos perpassados por conta do atual modelo tomado para utilização de softwares de gestão processual, a fim de que se oportunize o fornecimento de medidas preventivas eficazes em face de incidentes de segurança.

1.2 ASCENSÃO DO PROGRAMA DE GOVERNANÇA DIGITAL NO PJSC

Com a implantação do processo eletrônico no Tribunal de Justiça de Santa Catarina (TJSC) em janeiro de 2016, o Poder Judiciário de Santa Catarina (PJSC) concluiu o processo de informatização de seus procedimentos jurisdicionais, iniciado em 2006. Esse marco teve início com a implementação de uma nova versão do Sistema de Automação da Justiça de Primeiro Grau (SAJ/PG) no Juizado Especial Cível do Norte da Ilha de Florianópolis, situado no bairro de Santo Antônio de Lisboa, permitindo a tramitação integralmente digital dos processos judiciais naquela unidade jurisdicional¹¹⁰.

A adoção do meio digital para a tramitação de processos e a realização de atos processuais consolidou um novo paradigma operacional no PJSC. Essa transição implicou transformações significativas nas rotinas de trabalho, nos procedimentos de recepção, análise e julgamento dos feitos, bem como na gestão dos processos administrativos e jurisdicionais, promovendo uma reestruturação profunda na forma de atuação do Poder Judiciário¹¹¹.

¹¹⁰ ROSSA, Ramila. **Governança dos Sistemas Judiciais do Poder Judiciário de Santa Catarina**. Revista de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | Salvador | v. 4 | n. 1 | p. 72 – 91 | Jan/Jun. 2018.

¹¹¹ ROSSA, Ramila. **Governança dos Sistemas Judiciais do Poder Judiciário de Santa Catarina**. Revista de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | Salvador | v. 4 | n. 1 | p. 72 – 91 | Jan/Jun. 2018.

O paradigma atual de virtualização completa dos procedimentos jurisdicionais estabelece que os sistemas judiciais não se limitam a atuar como meras ferramentas de apoio à atividade-fim do Poder Judiciário de Santa Catarina (PJSC). Em vez disso, esses sistemas são concebidos como instrumentos essenciais para a efetivação do acesso à justiça, de modo que o sistema e suas funcionalidades passaram a constituir o próprio processo. Assim, o PJSC deixou de ser uma organização que simplesmente emprega tecnologia digital e transformou-se em uma organização intrinsecamente digital¹¹².

Considerando o contexto supramencionado, todas as atividades da organização (PJSC) se mostraram essenciais ao cumprimento da missão e visão do PJSC, qual seja, “realizar Justiça por meio da humanização e da efetividade na prestação adequada da solução de conflitos e —Ser reconhecido como um Judiciário eficiente, célere e humanizado”¹¹³.

Inclusive, é diante deste cenário não isolado, que a função da Tecnologia da Informação (TI) nas organizações tem se transformado de forma significativa, deixando de se resumir a uma “central de suporte”, limitada à prestação de serviços emergenciais e à manutenção operacional dos sistemas, para se consolidar como uma área de liderança estratégica. A TI passou a estabelecer parcerias com as unidades de negócios, colaborando ativamente no desenvolvimento e na execução do planejamento e da estratégia corporativa. O objetivo central dessa transformação é maximizar o valor agregado aos produtos e serviços oferecidos pela organização, alinhando a tecnologia às necessidades estratégicas da empresa¹¹⁴.

Neste aspecto, o Poder Judiciário como um todo é chefiado pelo Conselho Nacional de Justiça, tendo como ordem diretiva a Resolução nº 211/2015, a qual institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário, a qual objetiva o aprimoramento contínuo da melhoria da

¹¹² ROSSA, Ramila. **Governança dos Sistemas Judiciais do Poder Judiciário de Santa Catarina**. Revista de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | Salvador | v. 4 | n. 1 | p. 72 – 91 | Jan/Jun. 2018.

¹¹³ PODER JUDICIÁRIO DE SANTA CATARINA. **Missão e Visão**. Disponível em: <<https://www.tjsc.jus.br/missao-e-visao>>. Acesso em: 21 out. 2024.

¹¹⁴ GARTNER. **Key Issues For Business Process Management**. 2008. Disponível em: <https://www.gartner.com/en/documents/620810>. Acesso em: 15 out. 2024.

governança, gestão e infraestrutura de tecnologia da informação do Poder Judiciário¹¹⁵.

De acordo com a resolução, a implementação da Governança de Tecnologia da Informação (GTI) ocorrerá a partir do cumprimento dos objetivos estratégicos estabelecidos, em alinhamento com as Diretrizes Estratégicas de Nivelamento. Este processo será viabilizado por meio do aprimoramento dos mecanismos de Governança de Tecnologia da Informação e Comunicação (TIC). Os nove objetivos estratégicos delineados na resolução estão organizados em três perspectivas¹¹⁶:

Tabela 1 - Objetivos da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário

PERSPECTIVA	OBJETIVO
Recursos	Aperfeiçoar as competências gerenciais e técnicas de pessoal
	Prover infraestrutura de TIC apropriada às atividades judiciais e administrativas
	Aprimorar a gestão orçamentária e financeira
Processos Internos	Aperfeiçoar a governança e a gestão
	Aprimorar as contratações
	Promover a adoção de padrões tecnológicos
	Aprimorar e fortalecer a integração e a interoperabilidade de sistemas de informação
Resultados	Aprimorar a segurança da informação
	Primar pela satisfação dos usuários

Fonte: Conselho Nacional de Justiça¹¹⁷

A Resolução 211/2015 reflete a preocupação do Conselho Nacional de Justiça (CNJ) com o alinhamento entre a estratégia dos órgãos do Poder Judiciário e a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), estabelecendo a obrigatoriedade de elaboração dos Planos Estratégicos de Tecnologia da Informação e Comunicação (PETIC) e dos Planos

¹¹⁵CONSELHO NACIONAL DE JUSTIÇA. Resolução 211/2015. **Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

¹¹⁶CONSELHO NACIONAL DE JUSTIÇA. Resolução 211/2015. **Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

¹¹⁷ CONSELHO NACIONAL DE JUSTIÇA. Resolução 211/2015. **Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

Diretores de Tecnologia da Informação e Comunicação (PDTIC) por parte dos tribunais, sendo o elemento propulsor para a adoção das medidas¹¹⁸.

No âmbito do Poder Judiciário de Santa Catarina (PJSC), foi promulgada a Resolução 31, em 27 de junho de 2018, a qual institui o Comitê de Governança de Tecnologia da Informação e o Comitê de Gestão de Tecnologia da Informação, em conformidade com os preceitos da Resolução 211/2015 do CNJ¹¹⁹, revertendo-se no primeiro passo institucional dedicado ao aprimoramento da Governança Digital do Poder Judiciário de Santa Catarina.

A partir deste momento, o Poder Judiciário de Santa Catarina estabeleceu uma série de Resoluções destinadas ao contínuo desenvolvimento da governança digital do órgão, destacando-se as seguintes:

- Resolução GP n. 27/2024: Reestrutura o Comitê de Governança de Segurança da Informação e o Núcleo de Segurança Cibernética e dá nova denominação e reestrutura a Equipe de Prevenção, Tratamento e Resposta a Incidentes de Segurança Cibernética no âmbito do Poder Judiciário do Estado de Santa Catarina.
- Resolução TJ n. 50/2023: Institui a Política de Educação e Cultura em Segurança Cibernética no âmbito do Poder Judiciário do Estado de Santa Catarina.
- Resolução GP n. 11/2021: Institui a Política de Controle de Acesso aos Recursos e Serviços de Tecnologia da Informação no âmbito do Poder Judiciário do Estado de Santa Catarina e dá outras providências.
- Resolução GP n. 10/2021: Institui a Política de Uso do Correio Eletrônico Institucional no âmbito do Poder Judiciário do Estado de Santa Catarina e dá outras providências. COM A REDAÇÃO DADA PELO ART. 1º DA RESOLUÇÃO GP N. 25/2022
- Instrução Normativa DTI n. 01/2020: Fixa diretrizes para a operacionalização da Política de Senhas no âmbito do Poder Judiciário do Estado de Santa Catarina.
- Resolução GP n. 19/2020: Institui a Política de Senhas no âmbito do Poder Judiciário do Estado de Santa Catarina e dá outras providências.
- Resolução GP n. 28/2019: Institui o Comitê Gestor de Proteção de Dados no âmbito do Poder Judiciário do Estado de Santa Catarina¹²⁰.

Ainda que haja um extenso rol de documentos organizacionais, destacam-se as diretrizes estratégicas de Tecnologia da Informação (TI) do Poder

¹¹⁸ CONSELHO NACIONAL DE JUSTIÇA. Resolução 211/2015. **Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

¹¹⁹ SANTA CATARINA. Tribunal de Justiça. Resolução TJ n. 15, de 4 de julho de 2018. **Institui a Política de Segurança da Informação do Poder Judiciário do Estado de Santa Catarina e dá outras providências**. Disponível em: <https://busca.tjsc.jus.br/buscatextual/integra.do?cdSistema=1&cdDocumento=179376&cdCategoria=1>. Acesso em: 15 out. 2024.

¹²⁰ SANTA CATARINA. Tribunal de Justiça. **Legislação Relacionada**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/legislacao-relacionada>. Acesso em: 15 out. 2024.

Judiciário de Santa Catarina, definidas pelo Comitê de Governança de Tecnologia da Informação (CGOVTI), visam orientar as ações e projetos de TI, promovendo o alinhamento estratégico com os objetivos institucionais e a otimização do uso dos recursos disponíveis¹²¹.

A atual gestão (2022-2024) distribuiu as Diretrizes em múltiplas dimensões e eixos temáticos:

Tabela 2 – Diretrizes e Estratégias de Tecnologia da Informação

Dimensão	Eixo	Descrição
Institucional		Minimizar os riscos de continuidade do negócio por meio da implantação da governança e gestão da Segurança da Informação institucional, assim como da capacitação e conscientização contínua dos magistrados e servidores.
Tecnologia	Governança e Gestão de TI	Aperfeiçoar e normatizar as atividades, incrementando a padronização, a segurança e a produtividade.
Tecnologia	Governança e Gestão de TI	Compartilhar modelos e práticas bem-sucedidas.
Tecnologia	Segurança da Informação	Fortalecer a Segurança da Informação por meio da priorização de ações que mitiguem vulnerabilidades nos serviços de TIC.
Tecnologia	Segurança da Informação	Capacitação contínua das equipes de TI em Segurança da Informação.
Tecnologia	Sistemas Judiciais	Priorizar ações que aumentem a capacidade produtiva da DTI na evolução do eproc.
Tecnologia	Sistemas Judiciais	Promover a melhoria do sistema eproc com automatizações, IA e novas ferramentas para maior rendimento.

¹²¹ SANTA CATARINA, Tribunal de Justiça. **Diretrizes Estratégicas de Tecnologia da Informação**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/diretrizes-estrategicas-de-tecnologia-da-informacao>. Acesso em: 15 out. 2024.

Tecnologia	Inteligência Artificial	Utilizar IA de forma ética para reduzir tempo e custo dos processos e aumentar eficiência e segurança jurídica.
Tecnologia	Equipamentos de TI	Suspender a aquisição de impressoras até a conclusão do projeto de sustentabilidade e otimização.
Tecnologia	Equipamentos de TI	Promover a renovação dos equipamentos de informática.
Tecnologia	Sistemas Administrativos e de Apoio	Concentrar serviços selecionados em um único aplicativo para dispositivos móveis.
Tecnologia	Sistemas Administrativos e de Apoio	Racionalizar a força de trabalho por meio de atividades remotas e otimização de funções subaproveitadas.
Tecnologia	Sistemas Administrativos e de Apoio	Manter o site institucional atualizado, ampliando suas finalidades e tornando-o mais funcional.
Tecnologia	Sistemas Administrativos e de Apoio	Expandir serviços virtuais, como chatbots, para liberar o componente humano para outras atividades.
Tecnologia	Sistemas Administrativos e de Apoio	Criar repositório interno de sentenças e aprimorar bancos de dados para facilitar a identificação de temas repetitivos.

Fonte dos dados: Tribunal de Justiça de Santa Catarina¹²²

Atualmente, o cumprimento das diretrizes organizacionais e a fiscalização de todo o programa de Governança se encontra sob responsabilidade do Comitê de Governança de Tecnologia da Informação, este formado por magistrados e servidores e regido pela Resolução GP Nº 31/2018 e a Portaria GP Nº 317/2020¹²³.

¹²² SANTA CATARINA, Tribunal de Justiça. **Diretrizes Estratégicas de Tecnologia da Informação**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/diretrizes-estrategicas-de-tecnologia-da-informacao>. Acesso em: 15 out. 2024.

¹²³ SANTA CATARINA, Tribunal de Justiça. **Comitê de Governança de Tecnologia da Informação**. Disponível em: <https://www.tjsc.jus.br/orgaos-administrativos/comite-de-governanca-de-tecnologia-da-informacao>. Acesso em: 15 out. 2024.

1.2.1 PLANO ORÇAMENTÁRIO

A viabilidade de fornecer uma análise sólida à presente dissertação está diretamente ligada à previsão orçamentária destinada ao programa de governança digital do PJSC, muito embora a implantação de diretrizes e regramentos seja essencial, o projeto de governança seria frustrado diante de orçamentos insuficientes.

Percebe-se que em momento anterior aos regulamentos que instituíram o Comitê de Governança, sequer existia planejamento orçamentário acerca dos investimentos destinados à gestão da tecnologia da informação no PJSC, motivo pelo qual tal acompanhamento vem sendo realizado a partir do ano de 2019.

Gráfico 1 - Orçamento Tecnologia da Informação – Exercício 2019



Fonte: Tribunal de Justiça de Santa Catarina¹²⁴

Gráfico 2 – Orçamento Tecnologia da Informação PJSC 2020

¹²⁴ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2019.** Disponível em: <https://www.tjsc.jus.br/documents/840056/3546219/Or%C3%A7amento+e+Execu%C3%A7%C3%A3o+-+exerc%C3%ADcio+2019/55c3c2ce-71d8-bcce-3df8-e4404e2e7d23>. Acesso em: 15 out. 2024.


ORÇAMENTO TECNOLOGIA DA INFORMAÇÃO - EXERCÍCIO 2020
VALOR PROPOSTO: R\$ 76.329.623,86
EXECUÇÃO ORÇAMENTO TI - 2020 - CONTRATOS

Tema Orçamentário	EMPENHADO ATÉ 31/12/2020	TOTAL LIQUIDADO POR TITULO	LIQUIDADO												Restos a pagar
			Jan/20	Fev/20	Mar/20	Abr/20	Mai/20	Jun/20	Jul/20	Ago/20	Sep/20	Out/20	Nov/20	Dez/20	
Governança e gestão de TI	77.048,40	74.806,11	4.618,67	11.886,70	3.291,38	7.134,11	3.737,71	16.800,00	8.759,04	0,00	7.520,75	0,00	1.806,11	0,00	9.027,62
Gestão de Sistemas Administrativos	548.225,70	540.536,14	114.932,54	87.580,30	13.798,75	118.837,86	6.889,40	1.394,12	1.803,12	727,42	11.916,28	537,00	8.138,00	0,00	4.051,00
Segurança da Informação	703.873,27	693.773,27	9.784,10	205.546,65	232.751,41	145.186,79	1.326,63	0,00	0,00	0,00	0,00	0,00	0,00	0,00	56.838,67
Gestão de microinformática	4.115.373,82	4.108.762,82	388,47	484.997,13	185.511,09	8.344.124,60	86.136,61	4.827,30	22.224,21	948,85	980,34	13.798,97	40,64	13.225,50	0,00
Gestão de Sistemas Judiciais	48.066.456,80	48.734.764,71	0,00	459.823,75	459.225,85	413.757,69	11.189.405,73	8.202.863,67	3.213.811,89	4.838.548,19	3.537.821,80	3.505.865,90	1.948.548,84	3.103.551,38	11.029.372,12
Gestão de Telecomunicações	5.793.210,08	5.622.649,23	65.000,00	1.167.382,50	1.454.488,18	1.341.793,51	89.176,40	66.345,60	56.870,37	12.474,50	15.716,10	10.167,68	1.103.154,51	187.840,63	13.932,42
Gestão de Infraestrutura de TI	5.280.989,10	5.270.989,10	41.494,07	363.347,40	1.274.525,94	2.913.688,11	0,00	0,00	6.882,72	0,00	0,00	0,00	319.229,23	319.229,23	0,00
Total:	65.481.025,75	63.045.369,82	235.796,85	2.829.280,69	3.841.393,79	8.487.901,47	11.276.772,18	3.281.900,98	3.950.369,87	4.850.798,75	3.575.925,87	3.518.369,54	3.303.998,17	3.676.787,19	11.093.634,14
EXECUÇÃO ORÇAMENTÁRIA:	85,79%	82,60%	0,31%	4,81%	8,79%	29,91%	34,68%	38,99%	43,38%	49,68%	54,18%	58,80%	63,24%	68,06%	82,60%

Valor total do orçamento OTI com contingenciamento: 76.329.623,86

 Fonte: Tribunal de Justiça de Santa Catarina¹²⁵

Gráfico 3 - Orçamento Tecnologia da Informação PJSC – 2021

VALOR PROPOSTO: R\$ 99.932.800,00

 Fonte: Tribunal de Justiça de Santa Catarina¹²⁶

Gráfico 4 – Orçamento Tecnologia da Informação PJSC 2022

¹²⁵ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2020.** Disponível em: <https://www.tjsc.jus.br/documents/840056/3546219/Or%C3%A7amento+e+Execu%C3%A7%C3%A3o+-+2020/3a5eccd9-6d06-b959-6269-d0e1fdf74edb>. Acesso em: 15 out. 2024.

¹²⁶ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2021.** Disponível em: https://www.tjsc.jus.br/documents/840056/844731/Or%C3%A7amento+e+Execu%C3%A7%C3%A3o+-+2021_vers%C3%A3o+para+publica%C3%A7%C3%A3o_.pdf/0522d5e8-3ecb-ec2e-defc-87cd7fa10fe5?t=1673975043934. Acesso em: 15 out. 2024.



Fonte: Tribunal de Justiça de Santa Catarina¹²⁷

Gráfico 5 - Orçamento Tecnologia da Informação 2023



Fonte: Tribunal de Justiça de Santa Catarina¹²⁸

Gráfico 6 – Orçamento Tecnologia da Informação

¹²⁷ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2022.** Disponível em: <https://www.tjsc.jus.br/documents/840056/3546219/Or%C3%A7amento+e+Execu%C3%A7%C3%A3o+2022.pdf/41dae97c-04df-9f05-e50e-61183184a4be?t=1680644316606>. Acesso em: 15 out. 2024.

¹²⁸ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2023.** Disponível em: <https://tjscjusbr0.sharepoint.com/sites/DTI-Equipos/Arquivos%20da%20DTI/Forms/AllItems.aspx?id=%2Fsites%2FDTI%2DEquipos%2FArquivos%20da%20DTI%2FPortal%20Web%2FContrata%C3%A7%C3%B5es%20de%20TIC%2FExecu%C3%A7%C3%A3o%20Or%C3%A7ament%C3%A1ria%2FOr%C3%A7amento%20e%20Execu%C3%A7%C3%A3o%20de%20dezembro%20de%202023%20%2B%20RP%2Epdf&parent=%2Fsites%2FDTI%2DEquipos%2FArquivos%20da%20DTI%2FPortal%20Web%2FContrata%C3%A7%C3%B5es%20de%20TIC%2FExecu%C3%A7%C3%A3o%20Or%C3%A7ament%C3%A1ria&p=true&ga=1>. Acesso em: 15 out. 2024.



Fonte: Tribunal de Justiça de Santa Catarina ¹²⁹

O Planejamento Orçamentário de Tecnologia da Informação e Comunicação (TIC) está alinhado com o Planejamento Estratégico Institucional (PEI) e o Planejamento Estratégico e Diretor de TIC (PETIC/PDTIC) do Poder Judiciário de Santa Catarina (PJSC), em conformidade com a Lei de Responsabilidade Fiscal (LRF), a Lei de Diretrizes Orçamentárias (LDO) e o Plano Plurianual (PPA)¹³⁰.

O orçamento é submetido à aprovação do Comitê de Governança de TIC (CGesTI) antes de sua validação pelo Núcleo Financeiro do PJSC. Posteriormente, o plano é publicado e sua execução monitorada de forma contínua por meio do portal de TI institucional, a fim de acompanhamento dos valores distribuídos mensalmente até o fim do exercício¹³¹.

Percebe-se um vultuoso aumento orçamentário desde o exercício de 2019 do qual iniciou-se o acompanhamento, fator determinante em uma análise da qual confirma-se a crescente preocupação do PJSC em relação a transparência e segurança da informação da instituição.

¹²⁹ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2024**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/planejamento-orcamentario>. Acesso em: 17 out. 2024.

¹³⁰ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2024**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/planejamento-orcamentario>. Acesso em: 17 out. 2024.

¹³¹ SANTA CATARINA, Tribunal de Justiça. **Orçamento de Tecnologia da Informação – Exercício 2024**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/planejamento-orcamentario>. Acesso em: 17 out. 2024.

1.2.2 PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do Tribunal de Justiça de Santa Catarina (TJSC) é um instrumento estratégico que orienta o diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação e Comunicação (TIC). Trata-se de uma ferramenta essencial para a consecução das metas definidas no Planejamento Estratégico Institucional (PEI) e na Estratégia Nacional do Poder Judiciário (ENTIC-JUD)¹³².

A ENTIC-JUD por sua vez, tem como objetivo aprimorar a governança, a gestão e a colaboração tecnológica no âmbito do Judiciário, visando promover maior eficiência, eficácia, efetividade e economicidade nas operações dos órgãos, assegurando a otimização dos recursos disponíveis e a maximização dos resultados¹³³.

O PDTIC do TJSC abrange todas as unidades do Tribunal e estabelece uma série de princípios que são semestralmente revisados dos quais buscam o contorno dos desafios institucionais, sendo eles:

Tabela 3 – Princípios PDTIC PJSC

ID	Princípio	Referência
PR.001	80/20 - Não definir regras de sistema com base em situações excepcionais	DR.019
PR.002	Sempre primar pela simplicidade	DR.019
PR.003	Priorizar o conteúdo em detrimento da forma	DR.019
PR.004	A TI não fará o papel do negócio e vice-versa	DR.019
PR.005	Cordialidade no atendimento	DR.019
PR.006	Comunicação, comunicação, comunicação	DR.019
PR.007	Não criar urgências - planejamento e parcimônia	DR.019

¹³² SANTA CATARINA, Tribunal de Justiça. **Plano Diretor de Tecnologia da Informação e Comunicação**. Disponível em: <https://www.tjsc.jus.br/documents/840056/3742360/335+-+Plano+Diretor+de+TI+-+2022+%282%29.pdf/43bd052d-33d1-73d7-4eaf-5e95bba4cc9d?t=1670360563872>. Acesso em: 18 out. 2024.

¹³³ SANTA CATARINA, Tribunal de Justiça. **Plano Diretor de Tecnologia da Informação e Comunicação**. Disponível em: <https://www.tjsc.jus.br/documents/840056/3742360/335+-+Plano+Diretor+de+TI+-+2022+%282%29.pdf/43bd052d-33d1-73d7-4eaf-5e95bba4cc9d?t=1670360563872>. Acesso em: 18 out. 2024.

PR.008	Time DTI	DR.019
PR.009	Compartilhar conhecimento	DR.019
PR.010	Automatizar tudo o que for possível	DR.019
PR.011	Pequenas entregas - dividir para conquistar	DR.019
PR.012	Educação e inovação como alicerce fundamental para o fomento da cultura em segurança cibernética	DR.003
PR.013	Orientação à gestão de riscos e à gestão da segurança da informação	DR.003
PR.014	Prevenção, tratamento e resposta a incidentes cibernéticos	DR.003
PR.015	Articulação entre as ações de segurança cibernética e de proteção de dados e ativos de informação	DR.003
PR.016	Garantia ao sigilo das informações imprescindíveis à segurança da sociedade e do Estado e inviolabilidade da vida privada, da honra e da imagem das pessoas	DR.003
PR.017	Confidencialidade: garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal	DR.012
PR.018	Disponibilidade: garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido	DR.012
PR.019	Integridade: garante a não violação das informações para protegê-las contra alteração, gravação ou exclusão acidental ou proposital	DR.012
PR.020	Responsabilidade: atribui obrigações e deveres a pessoa que ocupa determinada função em relação ao acervo de informações	DR.012

Fonte: Tribunal de Justiça de Santa Catarina ¹³⁴

Percebe-se que os princípios estabelecidos seguem as melhores práticas de mercado marcadas pelos *frameworks* de governança digital e segurança

¹³⁴ SANTA CATARINA, Tribunal de Justiça. **Plano Diretor de Tecnologia da Informação e Comunicação.** Disponível em: <https://www.tjsc.jus.br/documents/840056/3742360/335+-+Plano+Diretor+de+TI+-+2022+%282%29.pdf/43bd052d-33d1-73d7-4eaf-5e95bba4cc9d?t=1670360563872>. Acesso em: 18 out. 2024.

da informação, princípios estes que norteiam o atual portfólio de projetos priorizados pelo CGovTI que a DTI estima no Plano Diretor concluir em sua vigência (2022-2024), quais sejam:

Tabela 4 – Projetos Priorizados CGovTI

Nome	Objetivos / Benefícios Esperados
Expansão do Portal de Serviços: Solicitação de demandas aos TSI do 1º Grau e do 2º Grau (Diretoria-Geral Judiciária, Corregedoria-Geral da Justiça e Academia Judicial).	Objetivo: Ter todos os atendimentos de primeiro nível (N1), realizados pelos técnicos de sistemas de informação (TSI), no Portal de Serviços. Benefícios esperados: - Unificação e padronização da abertura de chamados. - Revisão do catálogo de serviços e fluxo de atendimento. - Implantação do fluxo de gestão de ativos. - Gestão de todos os atendimentos e criação de indicadores de produtividade e qualidade.
Roadmap do Portfólio de Projetos: Projeto Piloto – Criação do roadmap dos projetos e projeto piloto na Divisão de Sistemas Administrativos (DSA).	Objetivo: Criar um modelo de visão consolidado em uma linha do tempo dos projetos de TIC, em andamento ou não iniciados, que são executados pela DSA. Benefícios esperados: - Obtenção de estimativas de início e conclusão dos projetos mais acuradas. - Promoção do alinhamento entre os gestores e as equipes. - Prestação de contas e transparência na execução dos projetos de TI.
Revisão dos critérios de priorização e seleção dos projetos de tecnologia da informação e comunicação.	Objetivo: Manter a legislação interna relacionada aos critérios de priorização e recebimento de demandas de solução de TI atualizada e em harmonia com as diretrizes da administração do PJSC. Benefícios esperados: - Promoção da seleção de projetos, evitando a entrada no portfólio de projetos que provavelmente não serão executados. - Racionalização dos recursos empregados na manutenção e atualização do portfólio de projetos e produtos de TI. - Otimização do processo de gerenciamento do portfólio com foco nas demandas que agregam valor ao PJSC.
Roadmap do Portfólio de Projetos: Aplicação do roadmap de projetos em toda a Diretoria de Tecnologia da Informação.	Objetivo: Aplicar o modelo definido no projeto piloto em toda DTI. Benefícios esperados: - Obtenção de estimativas de início e conclusão dos projetos mais acuradas. - Promoção do alinhamento entre os gestores e as equipes. - Prestação de contas e transparência na execução dos projetos de TI. - Respostas para as perguntas: Onde estamos? A onde queremos chegar? Como chegaremos? Quando chegaremos?
Implantação do processo de gestão do conhecimento.	Objetivo: Ter um repositório padronizado de conhecimento referente aos atendimentos de incidentes e às requisições por serviços de tecnologia da informação e comunicação. Benefícios esperados: - Formação de base de conhecimento necessária à implantação de ferramentas de autoatendimento e chatbots. - Universalização do conhecimento, facilitando a inserção de novos integrantes nas equipes de atendimento e promovendo a padronização dos atendimentos para demandas recorrentes.

Implantação da gestão de riscos de tecnologia da informação, alinhado à norma ABNT NBR ISO/IEC 31000.	<p>Objetivo: Ter um processo de gestão de riscos de TI plenamente implantado.</p> <p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Aumento da maturidade e capacidade de gerenciamento de riscos de TI, resultando na prestação dos serviços jurisdicionais com mais qualidade. - Identificação, priorização e tratamento dos riscos de TI com base em critérios técnicos objetivos em conformidade com a norma ABNT NBR ISO/IEC 31000. - Fornecimento de subsídios técnicos e objetivos para apoiar a tomada de decisão pelo corpo diretivo do PJSC. - Alocação seletiva de recursos e implementação de ações preventivas voltadas a evitar ou reduzir perdas na prestação dos serviços jurisdicionais suportados por ferramentas de TI. - Capacitação da equipe técnica para promoção da expertise em gestão de riscos de TI.
Implantação do processo de gerenciamento da grade de serviços de TI.	<p>Objetivo: Ter um processo de gerenciamento da grade de serviços plenamente implantado.</p> <p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Unificação e padronização da oferta de serviços de TIC. - Melhora da experiência dos usuários no consumo dos serviços de TIC. - Gerenciamento das ações de forma integrada na inclusão, alteração ou exclusão de serviços ofertados.
Programa de melhoria em governança, acessibilidade e usabilidade do Portal Institucional*.	<p>Objetivo: Ter normas e processos de trabalho definidos para evoluir e manter de forma consistente o portal institucional.</p> <p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Implantação de governança do portal institucional. - Melhora na usabilidade e na acessibilidade do Portal Institucional, seguindo boas práticas, recomendações e legislação correlata.
Criação de processo para gestão do Ciclo de Vida de Soluções de TIC do PJSC.	<p>Objetivo: Ter um processo de gerenciamento efetivo das soluções de TIC sob governança da DTI.</p> <p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Catálogo de soluções de software (Portfólio de Produtos) atualizado. - Priorização e seleção de demandas evolutivas, que compõem o backlog de melhorias dos produtos e serão desenvolvidas por equipe interna ou fábrica de software. - Utilização responsável dos recursos de TIC. - Oferta de soluções de TIC com maior qualidade para os usuários internos e externos. - Centralização das informações técnicas e documentação dos produtos gerenciados. - Promoção da sustentação das soluções de TIC.
Implantação do Sistema de Gestão de Segurança da Informação (SGSI), alinhado às normas ABNT NBR ISO/IEC 27001:2013 e às diretrizes da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).	<p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Elevar o nível de maturidade da governança em segurança da informação de TI. - Minimizar os riscos de interrupção dos serviços e sistemas em decorrência de ataques cibernéticos. - Desenvolver a resiliência e melhorar a capacidade de enfrentar eventos adversos relacionados a cibersegurança.
Implementação de uma camada adicional de segurança nos serviços disponibilizados via internet.	<p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Aumentar o nível de segurança e resiliência às ameaças externas dos sistemas e serviços online e que estão disponíveis na internet.
Implementação de uma solução de análise das vulnerabilidades na infraestrutura de servidores de rede e aplicações.	<p>Objetivo: Conhecer e mitigar os riscos e ameaças de segurança da informação nos serviços online.</p>
Desligamento dos servidores de rede de comarcas.	<p>Benefícios esperados:</p> <ul style="list-style-type: none"> - Aumentar a disponibilidade de serviços aos usuários das comarcas. - Desonerar as atividades dos TSI na gestão destes equipamentos e reduzir custos de aquisição e manutenção de equipamentos.

Atualização dos sistemas operacionais de servidores de rede do parque tecnológico.	Benefícios esperados: - Mitigar os riscos e ameaças de segurança da informação em serviços desatualizados ou não utilizados. - Liberar a infraestrutura para uso em novos serviços.
Modernização de toda a infraestrutura de backup de dados.	Benefícios esperados: - Atualizar para as tecnologias mais recentes a realização de cópias de segurança e proteção de dados do PJSC. - Mitigar riscos e ameaças de segurança da informação.
Desligamento da infraestrutura legada, que será substituída pelo sistema ERP.	Benefícios esperados: - Mitigar os riscos e ameaças de segurança da informação em serviços desatualizados ou não utilizados. - Liberar a infraestrutura para uso em novos serviços.
Atualização dos serviços de aplicação disponibilizados na internet.	Benefícios esperados: - Mitigar os riscos e ameaças de segurança da informação em serviços desatualizados ou não utilizados. - Liberar a infraestrutura para uso em novos serviços.
Atualização da infraestrutura do sistema Pergamum.	Benefícios esperados: - Mitigar os riscos e ameaças de segurança da informação em serviços desatualizados ou não utilizados. - Liberar a infraestrutura para uso em novos serviços.

Fonte: Tribunal de Justiça de Santa Catarina¹³⁵

O fator determinante do qual busca-se extrair a partir da análise dos projetos que estão sendo implementados resume-se na vultuosa quantidade de ações destinadas exclusivamente à segurança da informação, de forma que o PDTIC, em nenhum de seus projetos, prevê a utilização da tecnologia de *blockchain* em seu benefício.

Ainda que o PDTIC não preveja a utilização de *blockchain* em um projeto exclusivo destinado ao aprimoramento das medidas de segurança da informação, o TJSC, em seu Plano de Transformação Digital (PTD) dispõe sobre a atual integração da receita federal para consulta de pessoas junto ao novo modelo de integração *blockchain* da SERPRO, fator que desencadeia o primeiro passo acerca da implementação da tecnologia na instituição, ainda que ocorra em caráter de cooperação.

¹³⁵ SANTA CATARINA, Tribunal de Justiça. **Plano Diretor de Tecnologia da Informação e Comunicação.** Disponível em: <https://www.tjsc.jus.br/documents/840056/3742360/335+-+Plano+Diretor+de+TI+-+2022+%282%29.pdf/43bd052d-33d1-73d7-4eaf-5e95bba4cc9d?t=1670360563872>. Acesso em: 18 out. 2024.

1.2.3 LEVANTAMENTO DE GOVERNANÇA, GESTÃO E INFRAESTRUTURA DE TIC DO PJSC

Conforme exposto anteriormente, a Estratégia Nacional de Tecnologia da Informação e Comunicação (ENTIC-JUD), instituída pelo Conselho Nacional de Justiça (CNJ) por meio da Resolução nº 211/2015, estabeleceu diretrizes para o período de 2015 a 2020. O artigo 32 dessa resolução determina a realização de diagnósticos anuais com o objetivo de aferir o nível de cumprimento das Diretrizes Estratégicas de Nivelamento e, conseqüentemente, a evolução dos viabilizadores relacionados à Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação (TIC) no âmbito do Poder Judiciário¹³⁶.

Para avaliar o nível de maturidade nesses aspectos, Conselho Nacional de Justiça (CNJ), em conformidade com o Art. 11 da Resolução CNJ nº 370/2021 (ENTIC-JUD), realiza, anualmente, um diagnóstico para avaliar o nível de maturidade em Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação (TIC) dos órgãos sujeitos ao seu controle administrativo e financeiro¹³⁷.

Esse diagnóstico é operacionalizado por meio da aplicação do Índice de Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação do Poder Judiciário (iGovTIC-JUD), o qual é composto por perguntas e itens elaborados em conformidade com as diretrizes estratégicas de TIC definidas na Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)¹³⁸.

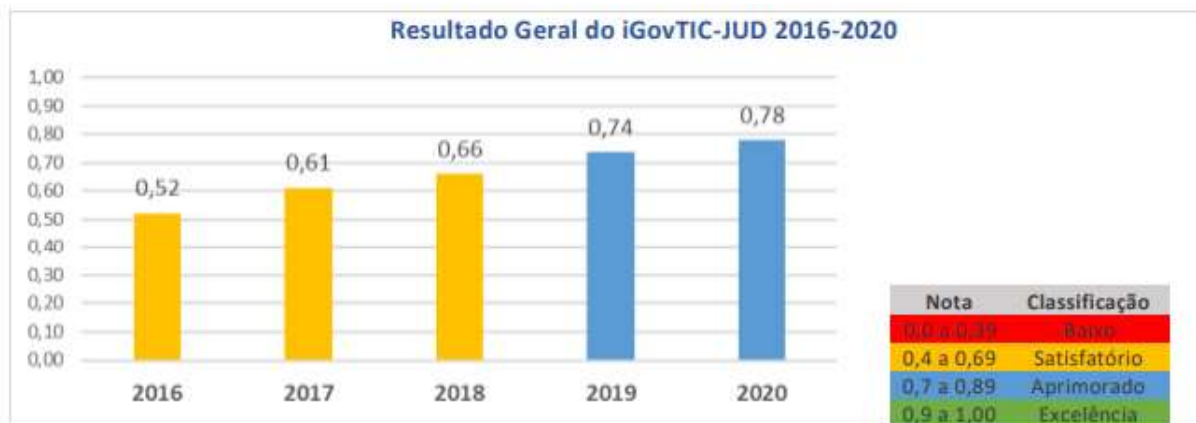
¹³⁶ CONSELHO NACIONAL DE JUSTIÇA. Resolução 211/2015. **Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

¹³⁷ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 370, de 28 de janeiro de 2021**. Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3706>. Acesso em: 15 out. 2024.

¹³⁸ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 370, de 28 de janeiro de 2021**. Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3706>. Acesso em: 15 out. 2024.

A primeira aplicação desse questionário eletrônico ocorreu em 2016, sob a denominação “Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário – iGovTIC-JUD”¹³⁹:

Gráfico 7 – Resultado IGOVTICJUD 2016-2020



Fonte: Conselho Nacional de Justiça¹⁴⁰

Os resultados preliminares indicam uma evolução considerável nos índices de maturidade das áreas de TIC dos órgãos do Poder Judiciário, essa tendência positiva é evidenciada no gráfico apresentado, que demonstra o crescimento da média geral do iGovTIC-JUD ao longo dos anos em que o levantamento foi realizado.

Muito embora tenham sido expostas dezenas de medidas adotadas pelo PJSC em matéria de governança de tecnologia da informação, o último relatório elaborado pelo CNJ aponta o órgão na 25ª colocação dentre 31 tribunais de médio porte:

Gráfico 7 – Resultado IGOVTICJUD 2016-2020

¹³⁹ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2018**. Disponível em: <https://www.tjsc.jus.br/documents/840056/4196365/Levantamento+iGovTIC-Jud+2018+-+Resultado+CNJ/1109afbd-1624-6eab-1c1e-1cf0bf24a2c6>. Acesso em: 18 out. 2024.

¹⁴⁰ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2023**. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/10/relatorio-geral-do-igovtic-jud-2023-2023-09-27-v2.pdf>. Acesso em: 18 out. 2024.

5.9 Resultados Geral iGovTIC-JUD 2023 – Órgãos de Médio Porte

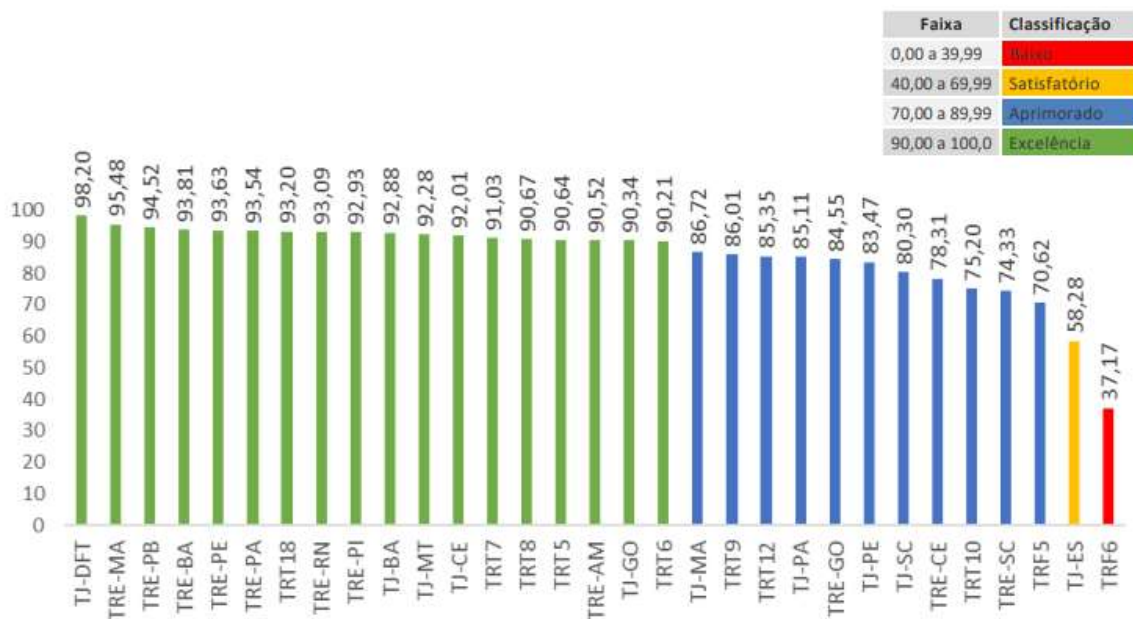


Gráfico 11. Classificação dos Órgãos de Médio Porte iGovTIC-JUD 2023

Fonte: Conselho Nacional de Justiça¹⁴¹

Fato igualmente curioso é que o PJSC sequer divulga os resultados dos últimos 5 (cinco) anos, ocasião que vai na contramão do princípio da transparência, um dos principais em matéria de governança digital¹⁴².

Ademais, atualmente, o quadro de medição em tempo real aponta que o PJSC se encontra na posição 67^a de 92 órgãos analisados anualmente acerca da maturidade em governança tecnológica¹⁴³.

Destaca-se que, apesar da melhoria observada ao longo dos anos, o PJSC ainda possui um amplo espaço para aprimorar a maturidade do programa de

¹⁴¹ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2023**. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/10/relatorio-geral-do-igovtic-jud-2023-2023-09-27-v2.pdf>. Acesso em: 18 out. 2024.

¹⁴² TRIBUNAL DE JUSTIÇA DE SANTA CATARINA (TJSC). **Resultados do iGovTIC-JUD**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/resultados-do-igovtic-jud>. Acesso em: 18 out. 2024.

¹⁴³ Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=36047c1e-acf8-4030-8474-78a20bae7c96&sheet=31049d4e-a530-4902-b1ed-6cb77477d5fa&theme=cnj_theme&select=Ano,2024

governança, caminho do qual de fato, só é possível trilhar a partir da análise de relatórios e dados firmados anualmente, os quais destacam os pontos de melhoria que podem ser adotados.

Capítulo 2

A UTILIZAÇÃO DE *BLOCKCHAIN* COMO MEDIDA DE PREVENÇÃO À INCIDENTES DE SEGURANÇA

2.1 ENTENDENDO A OPERACIONALIZAÇÃO DA *BLOCKCHAIN*

O surgimento de novas tecnologias é abarcado pela presença de vulnerabilidades e um conceito de inexistência da segurança plena sob o resguardo dos dados.

Nesse sentido, a tecnologia *Blockchain*, frequentemente associada às criptomoedas, tem um potencial transformador que se estende muito além do universo financeiro. No contexto do Judiciário, a *Blockchain* apresenta-se como uma ferramenta poderosa para a construção de um sistema mais eficiente, transparente e seguro.

A afirmação supramencionada encontra respaldo nas previsões do §1º e caput, art. 46 da LGPD, os determinam a necessidade de aplicação de medidas de segurança e a eventual aplicação de padrões técnicos mínimos, no entanto, em nenhum momento obrigam os agentes de tratamento ao pleno e expresso dever de garantir a segurança das informações (BRASIL, 2018).

Em que pese a atual maleabilidade regulatória, o mercado tecnológico buscou desenvolver tecnologias robustas aptas a resguardar as informações, tal como no caso prático da *blockchain* aplicada às criptomoedas.

Godoy¹⁴⁴ exprime que a aplicação da *blockchain* rouba olhares internacionais, tendo em vista que ela viabiliza a imutabilidade de informações de

¹⁴⁴ GODOY, Maria. *Blockchain* aplicada aos contratos inteligentes: perspectivas empresariais e natureza jurídica. In: LIMA, Ana Paula M. **Direito digital: Debates contemporâneos**. São Paulo: Thompson Reuters Brasil, 2019.

forma *online* no formato de um “livro-registro”, o qual enaltece a transparência e legitimidade dos dados.

A *blockchain* constitui um livro-razão distribuído, transparente e persistente, no qual apenas é possível adicionar novos registros, agrupados em blocos. Esse livro-razão distribuído permite a realização de transações confiáveis entre participantes não confiáveis¹⁴⁵.

Um conceito fundamental da *blockchain* é a transação, o termo “transação” foi inicialmente utilizado no contexto da primeira *blockchain* criada, o Bitcoin. Dado que o Bitcoin foi desenvolvido para fornecer soluções no âmbito financeiro, é possível empregar o termo “registro” para se referir às transações em aplicações não financeiras¹⁴⁶.

Um registro consiste em uma coleção de dados. Esses registros formam blocos, e os blocos, por sua vez, formam uma cadeia, originando o termo “*blockchain*”. Cada bloco contém uma marca temporal (timestamp) e um hash do bloco anterior na cadeia. Para que um novo bloco seja adicionado à *blockchain*, cada registro contido nele deve ser previamente validado. Esse processo de validação assegura a legalidade dos registros e, conseqüentemente, dos blocos¹⁴⁷.

As entidades que participam do armazenamento distribuído de dados compõem uma rede de nós (nodes), esses nós são entidades computacionais que se comunicam entre si para completar transações¹⁴⁸.

¹⁴⁵ Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M Parizi, and Kim-Kwang Raymond Choo. **A systematic literature review of *blockchain* cyber security**. Digital Communications and Networks, 2019.

¹⁴⁶ Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M Parizi, and Kim-Kwang Raymond Choo. **A systematic literature review of *blockchain* cyber security**. Digital Communications and Networks, 2019.

¹⁴⁷ Parth Thakkar, Senthil Nathan, and Balaji Viswanathan. Performance Benchmarking and Optimizing Hyperledger Fabric *Blockchain* Platform. In IEEE 26th International Symposium on Modeling, **Analysis, and Simulation of Computer and Telecommunication Systems**, pages 264–276, 2018.

¹⁴⁸ Uchi Ugobame Uchibeke, Sara Hosseinzadeh Kassani, Kevin A Schneider, and Ralph Deters. **Blockchain access control Ecosystem for Big Data security**. Green Computing and Communications (GreenCom), IEEE/ACM Int’l Conference on & Int’l Conference on Cyber, Physical and Social Computing, 2018.

Diversas *blockchains* podem utilizar diferentes algoritmos de consenso e mecanismos de recompensa, especialmente em *blockchains* permissionless, que dependem da contribuição de nós anônimos para manter o ecossistema. De modo geral, a tecnologia *blockchain* oferece um conjunto de propriedades que garantem integridade, autenticidade, transparência, rastreabilidade e auditabilidade, características atrativas para a resolução de problemas específicos¹⁴⁹.

A tecnologia *blockchain* não se limita a ser uma alternativa aos bancos centralizados, mas também possibilita novas arquiteturas, podendo atuar como um conector de software¹⁵⁰.

Além disso, para a plena compreensão do conceito, denota que o próprio nome “cadeia de blocos” insinua o formato de aplicação. Em suma, cada bloco abarca uma quantidade “X” de informações atinentes às mudanças incorridas em um período “Y”, após a formação do bloco ele é inserido na cadeia.

Tal movimento ocorre repetidamente até que haja a formação de uma “cadeia de blocos”, de forma que com uma quantidade considerável de blocos formados as informações tornam-se imutáveis, pois torna-se necessário desassociar todos os blocos de toda a cadeia, gerando a necessidade uma capacidade de processamento inexistente até o momento.

A imutabilidade e confiança das informações ganha relevância por conta da aplicação de criptografia em *hash*, a qual gera uma chave criptográfica atribuída a cada bloco, igualmente utilizada para a valoração do valor do *hash* do próximo bloco, gerando o elo entre os blocos, como preceitua Gupta¹⁵¹.

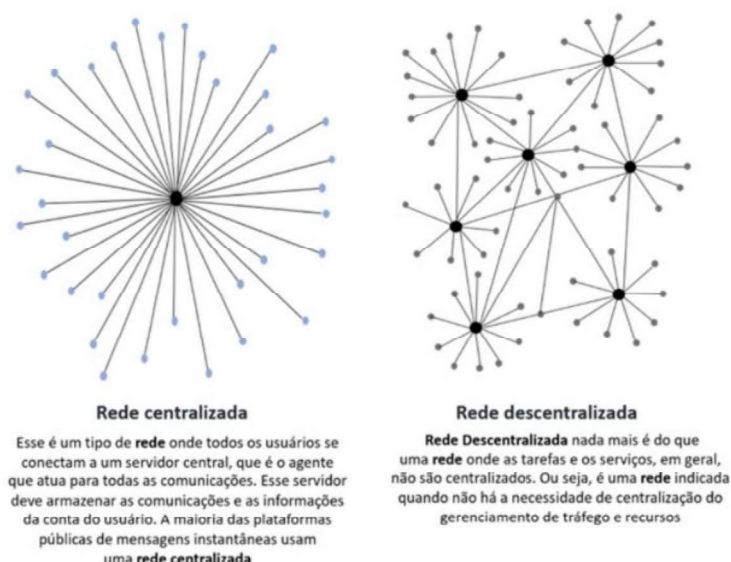
¹⁴⁹ Hai Wang, Yong Wang, Zigang Cao, Zhen Li, and Gang Xiong. **An Overview of Blockchain Security Analysis**. In *Cyber Security*, pages 55–72, 2019.

¹⁵⁰ Xiwei Xu, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, and Shiping Chen. **The Blockchain as a Software Connector**. In *13th Working IEEE/IFIP Conference on Software Architecture*, pages 182–191, 2016.

¹⁵¹ GUPTA, Ruchi. **Se você entender a função da Hash, você entenderá a Blockchain**. Disponível em: <https://guiadobitcoin.com.br/noticias/se-voce-entender-a-funcao-da-hash-voce-entendera-a-blockchain/>. Acesso em: 19 out. 2023.

Noutro ponto, torna-se cabal destacar que a operação obstinada da utilização da *blockchain* no Poder Judiciário de Santa Catarina é composto pelo conceito de uma rede Centralizada, destacada a seguir:

Figura 1 – Exemplo de “Nós” em redes centralizadas e descentralizadas



152

Fonte: elaborado por Cynthia Barbosa de Almeida e Anne Chang¹⁵³

Nesta modalidade, o “nó central”, no caso em questão o PJSC, é o controlador das operações, sendo o único usuário com permissões privilegiadas de verificação, validação e operacionalização das transações dos demais usuários não permissionados, seria o caso de um banco em relação aos seus clientes.

A descentralização é uma das características mais típicas e o conceito central do *blockchain*, em um ambiente com informações assimétricas e incertas, o *blockchain* cria um sistema de consenso de credibilidade de forma descentralizada e sem a necessidade de confiança em terceiros, utilizando algoritmos matemáticos em uma rede composta por nós desconhecidos¹⁵⁴.

¹⁵² CHANG, Anne; ALMEIDA, Cynthia Barbosa de. *Blockchain* e proteção de dados. In: PALHARES, Felipe. **Temas atuais de Proteção de Dados**. São Paulo: Thompson Reuters Brasil, 2020. Cap. 3.

¹⁵³ CHANG, Anne; ALMEIDA, Cynthia Barbosa de. *Blockchain* e proteção de dados. In: PALHARES, Felipe. **Temas atuais de Proteção de Dados**. São Paulo: Thompson Reuters Brasil, 2020. Cap. 3.

¹⁵⁴ Zou, J., Yu, B., Zhuang, P. and Xing, C. (2018), **Blockchain: Core Technologies and Applications**, China Machine Press, Beijing.

Cheng e Almeida¹⁵⁵ porventura destacam a possibilidade inovadora de uma “Rede Distribuída” da qual o “nó central” de responsabilidade do controlador pode determinar a diversas partes cópias do *ledger*¹⁵⁶, ou seja, a informação não resta sob responsabilidade de apenas um ente, o registro coletivo poderia ser eventualmente compartilhado a uma cadeia geral de controle de todo o Poder Judiciário do Brasil ou da eventual hierarquia ramificada escolhida.

Em suma, a *Blockchain* pode ser definida como um livro-razão digital, distribuído e imutável, que registra transações em blocos encadeados criptograficamente.

As principais características da *Blockchain* se resumem em: a) Descentralização: a *Blockchain* não depende de um servidor central, sendo distribuída em uma rede de computadores, o que garante maior resiliência e segurança; b) Imutabilidade: Uma vez registrada na *Blockchain*, a informação não pode ser alterada ou excluída, garantindo a integridade dos dados; c) Transparência: todas as transações registradas na *Blockchain* são visíveis a todos os participantes da rede, promovendo a transparência e a auditabilidade; e d) Segurança: a criptografia garante a segurança das transações e a integridade dos dados, protegendo contra fraudes e adulterações.¹⁵⁷

2.2 BENEFÍCIOS DA APLICAÇÃO DA *BLOCKCHAIN*

Conforme descrito no relatório do Tribunal de Contas da União¹⁵⁸, a aplicação da *blockchain* no setor público apresenta notórios avanços, tal como no caso da troca de dados entre países do Mercosul experimentada pela Receita Federal do Brasil e medida de contingência aplicada ao Sistema Alternativo de Transações

¹⁵⁵ CHANG, Anne; ALMEIDA, Cynthia Barbosa de. *Blockchain* e proteção de dados. In: PALHARES, Felipe. **Temas atuais de Proteção de Dados**. São Paulo: Thompson Reuters Brasil, 2020. Cap. 3.

¹⁵⁶ Trata-se de uma “lista criptografada de lançamentos e operações”.

¹⁵⁷ GALERY, Augusto Dutra; ALBERTIN, Alberto Luiz. Inclusão Digital. In: ALBERTIN, Alberto Luiz; MOURA, Rosa Maria (Org.). **Tecnologia da Informação**. 1. ed. 2. reimp. São Paulo: Atlas, 2007, pp. 242-254.

¹⁵⁸ BRASIL. Tribunal de Contas da União. **Levantamento da tecnologia *blockchain***. Brasília: TCU, Secretaria da Sessões (Seses), 2020.

pelo Banco Central do Brasil como medida de contingência para o caso de panes no sistema.

Sob a ótica do poder judiciário, a tecnologia *Blockchain* pode ser aplicada em várias áreas do Judiciário, oferecendo soluções inovadoras que permitem a otimização dos procedimentos, o aumento da segurança e a promoção da transparência nos processos judiciais¹⁵⁹.

Noutro ponto relevante, parte da doutrina defensora da implementação do *blockchain* no sistema jurídico moderno busca repensar a justiça no século XXI¹⁶⁰.

A título de exemplo, Ast e Sewrjugin argumentam que a revolução digital transformou muitas indústrias e instituições sem, no entanto, afetar o sistema jurídico de forma significativa¹⁶¹.

De acordo com o artigo de Ast e Sewrjugin os desenvolvimentos recentes em inteligência coletiva, governo aberto, epistemologia social e tecnologia *blockchain* devem levar a mudanças significativas em como os tribunais operam, tornando-os financeiramente sustentáveis e mais eficientes¹⁶².

2.2.1 Auditoria de Eventos

Noutra seara, a *blockchain* permitiria a coleta, o armazenamento e a gestão de provas digitais de forma muito segura e transparente. Ao registrar essas provas na *Blockchain*, garante-se a autenticidade e integridade, dificultando qualquer tipo de fraude ou manipulação de evidências. Isso é especialmente útil em casos que

¹⁵⁹ GALERY, Augusto Dutra; ALBERTIN, Alberto Luiz. Inclusão Digital. In: ALBERTIN, Alberto Luiz; MOURA, Rosa Maria (Org.). **Tecnologia da Informação**. 1. ed. 2. reimp. São Paulo: Atlas, 2007, pp. 242-254.

¹⁶⁰ Dylag M, Smith H (2021) **From cryptocurrencies to cryptocourts: Blockchain and the financialization of dispute resolution platforms**. Inf Commun Soc. <https://doi.org/10.1080/1369118X.2021.1942958>.

¹⁶¹ Ast F, Sewrjugin A (2015) **The crowdjury, a crowdsourced justice system for the collaboration era**. Crowdjury Org 1(9):1689–1699

¹⁶² Ast F, Sewrjugin A (2015) **The crowdjury, a crowdsourced justice system for the collaboration era**. Crowdjury Org 1(9):1689–1699.

envolvem provas digitais, como e-mails, arquivos de áudio, vídeos e outros tipos de dados eletrônicos que necessitam de proteção contra adulterações¹⁶³.

Ocorre que, processos de auditoria utilizam esses arquivos para tratar da validação, atribuição e produção de evidências.

A fase de validação verifica se o sujeito agiu conforme o esperado, a atribuição identifica o sujeito que não está em conformidade com o sistema, a fase de evidências produz provas não-repudiáveis que sustentam a atribuição para que os auditores possam reconstruir a sequência de ações realizadas por um usuário em um sistema, logo é uma necessidade que os logs de auditoria ofereçam garantias de integridade¹⁶⁴.

Os esquemas convencionais de proteção de dados incluem o uso de sistemas com modelos de segurança fracos, que operam com a suposição de que o site de registro não pode ser comprometido, no entanto, atacantes têm explorado essas fragilidades, destacando as ameaças à integridade dos dados¹⁶⁵.

A adulteração de arquivos de logs é uma dessas ameaças de alta relevância, visto que pode comprometer auditorias, tornando os dados não confiáveis.

Além disso, essa violação permite que o atacante, apague seus rastros, portanto, a integridade dos dados de logs de aplicação é crucial, tornando fundamental o uso de mecanismos que distribuam a confiança nessa integridade¹⁶⁶.

¹⁶³ GREMBERGEN, Wim van; DE HAES, Steven. **Implementing Information Technology Governance: models, practices, and cases**. IGI Publishing, 2008.

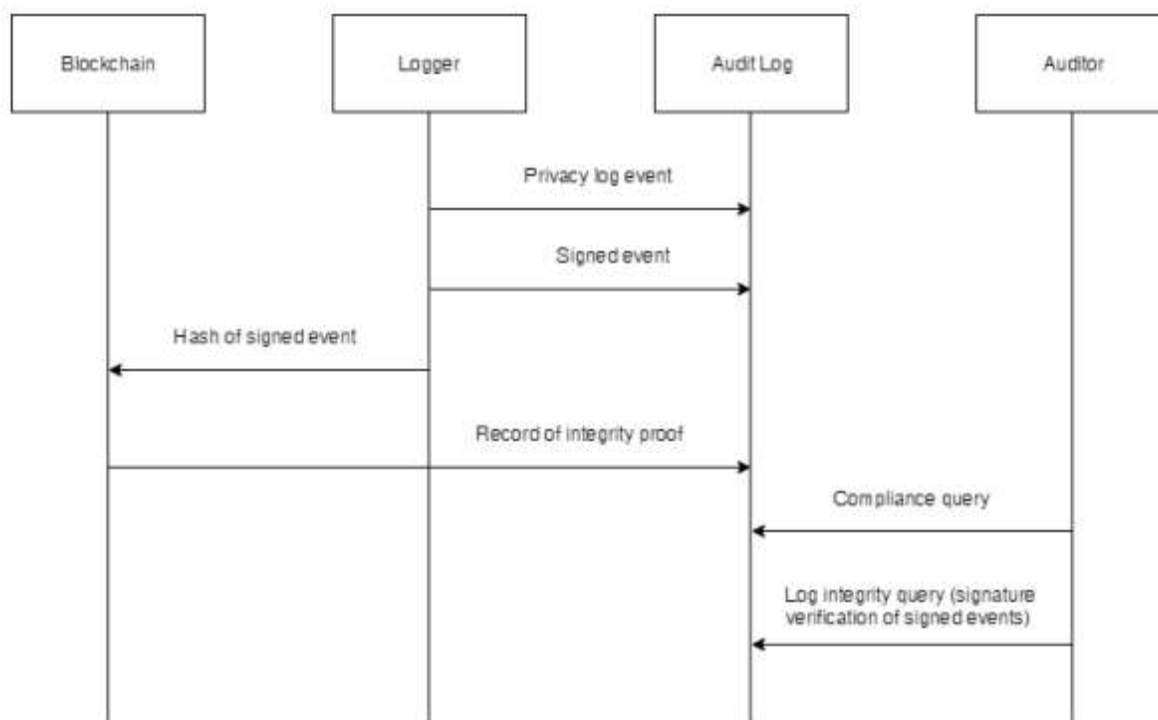
¹⁶⁴ Richard T Snodgrass, Shilong Stanley Yao, and Christian Collberg. **Tamper Detection in Audit Logs**. In 13th International Conference on Very Large Data Bases, VLDB '04, pages 504–515, 2004.

¹⁶⁵ Jonathan Margulies. **A Developer's Guide to Audit Logging**. IEEE Security Privacy, 13 (3):84–86, 2015.

¹⁶⁶ Laurent Maryline, Kaaniche Nesrine, and Le Christian. **A Blockchain based Access Control Scheme**. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, pages 168–176, 2018.

A *blockchain* emergiu como uma tecnologia que promete avanços não apenas na integridade dos dados, mas também em sua disponibilidade e não-repudiabilidade, características desejáveis para logs de aplicação¹⁶⁷.

Figura 2 – Exemplo de auditabilidade em logs de registro



Fonte: Andrew Sutton e Reza Samavi¹⁶⁸

Alguns autores estão explorando a tecnologia *blockchain* para criar logs de auditoria à prova de adulteração, Sutton e Samavi propõem um mecanismo de verificação de integridade e autenticidade de logs, que pode ser utilizado por auditores, utilizando o Bitcoin.

O sistema proposto registra provas de integridade na *blockchain*. O sistema envolve três entidades principais: o registrador, o log de auditoria e o auditor. O registrador cria os logs e os armazena no log de auditoria. Os auditores consultam

¹⁶⁷ Jordi Cucurull and Jordi Puiggalí. **Distributed Immutabilization of Secure Logs**. In Gilles Barthe, Evangelos Markatos, and Pierangela Samarati, editors, Security and Trust Management, pages 122–137, Cham, 2016.

¹⁶⁸ Andrew Sutton and Reza Samavi. **Blockchain Enabled Privacy Audit Logs**. In The Semantic Web – ISWC 2017: 16th International Semantic Web Conference, pages 645–660, 2017.

o log de auditoria, que contém os registros criados pelo registrador. Como os eventos precisam ser irrefutáveis, o registrador assina as transações, submetendo-as para provar a responsabilidade. Além disso, os logs precisam oferecer garantias de integridade, então provas de integridade (i.e., hash criptográfico) são geradas e armazenadas na *blockchain*¹⁶⁹.

2.2.2 Contratos Inteligentes (*Smart Contracts*)

Em uma área mais debatida, a *Blockchain* também viabiliza a criação de contratos inteligentes, ou smart contracts, que são contratos autoexecutáveis com cláusulas registradas em código. Esses contratos são executados automaticamente quando determinadas condições são cumpridas, o que agiliza processos e reduz a necessidade de intervenção humana. No Judiciário, eles podem ser usados na execução de sentenças ou acordos judiciais, otimizando o tempo e aumentando a eficiência dos procedimentos legais¹⁷⁰.

Em um cenário tecnológico e jurídico em constante evolução, as definições conceituais de termos e analogias estão em permanente transformação. O conceito de contrato inteligente não é exceção a essa dinâmica, a definição mais antiga de um contrato inteligente remonta ao artigo de Nick Szabo, publicado em 1996, definindo um contrato tradicional como "um conjunto de promessas acordadas por consenso, com o intuito de formalizar uma relação", enquanto o contrato inteligente fora destacado como "um conjunto de promessas, especificadas em formato digital, que incluem protocolos dentro dos quais as partes cumprem as referidas promessas"¹⁷¹.

Outra definição amplamente aceita de contratos inteligentes é apresentada por Christopher D. Clack, traduzindo um contrato inteligente como "um

¹⁶⁹ Andrew Sutton and Reza Samavi. **Blockchain Enabled Privacy Audit Logs**. In The Semantic Web – ISWC 2017: 16th International Semantic Web Conference, pages 645–660, 2017.

¹⁷⁰ GREMBERGEN, Wim van; DE HAES, Steven. **Implementing Information Technology Governance: models, practices, and cases**. IGI Publishing, 2008.

¹⁷¹ SZABO, Nick. **Smart Contracts: Building Blocks for Digital Markets. 1996**. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em 12 de nov. 2024.

acordo cuja execução é tanto automatizável quanto exigível. Automatizável por um computador, embora algumas partes possam requerer intervenção e controle humanos. Exigível mediante imposição legal de direitos e obrigações ou por meio de uma execução à prova de adulteração", essa definição reconhece que a formulação do contrato e a inserção do código requerem a intervenção cognitiva humana, enquanto a execução do contrato inteligente é automatizada com base em parâmetros preestabelecidos, garantindo o controle sobre os elementos essenciais à sua execução¹⁷².

Smart contracts não são contratos redigidos em linguagem jurídica, mas sim um conjunto de códigos incorporados ao sistema de *blockchain*, projetados para ajudar na execução dos acordos firmados entre os diferentes participantes. Desde que os códigos legíveis por máquina estejam escritos no smart contract, o sistema garante que eles sejam executados automaticamente assim que os protocolos pré-definidos forem ativados. Esses contratos são irrevogáveis, à prova de adulteração e independentes de terceiros¹⁷³.

O exemplo mais simples de um contrato inteligente na vida real é ilustrado por Szabo, por meio da analogia com uma máquina de venda automática. Quando o pagamento é efetuado, uma série de ações irreversíveis é desencadeada, e a máquina executa os termos do acordo, calculando e fornecendo o produto selecionado e o troco correspondente. Esse modelo se assemelha em muitos aspectos ao funcionamento de um contrato inteligente¹⁷⁴.

Para o caso em concreto, a *Blockchain* poderia ser empregada para a notariação e o registro de documentos em meio aos sistemas do PJSC, garantindo sua autenticidade e validade legal. Documentos registrados na *Blockchain* têm sua existência e integridade verificadas de maneira instantânea e indiscutível, sendo

¹⁷² BAKSHI, Vikram A.; BRAINE, Lee; CLACK, Christopher Clack. **Smart Contract Templates: Foundations, design landscape and research directions**. Aug. 4, 2016. Disponível em: https://www.researchgate.net/publication/305779577_Smart_Contract_Templates_foundation_s_design_landscape_and_research_directions_CDClack_VABakshi_and_LBraine_arxiv160800771_2016/link/5924238ea6fdcc4443ff2f6a/download. Acesso em 19 out. 2024.

¹⁷³ Ling, L. (2019), **Deconstruction of Blockchain**, Tsinghua University Publishing House, Beijing.

¹⁷⁴ SZABO, Nick. **Smart Contracts: Building Blocks for Digital Markets**. 1996. Disponível em: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em 19 out. 2024.

extremamente útil para certificados, testamentos, registros de propriedade e outros documentos importantes que requerem uma verificação segura e confiável¹⁷⁵.

2.2.3 Gerenciamento de Acessos

Em relação ao próprio login e identificação de servidores, peritos e advogados, a *Blockchain* permitiria a criação de sistemas extremamente seguros e confiáveis para o gerenciamento de identidades. Isso assegura a autenticidade e a segurança das informações de magistrados, servidores, advogados e outras partes envolvidas em processos judiciais, prevenindo fraudes e acessos indevidos, protegendo tanto os profissionais quanto as partes dos processos¹⁷⁶.

Resta quase cristalino que a implementação da tecnologia *Blockchain* no Judiciário pode trazer diversos benefícios significativos¹⁷⁷.

Isto porque a automação de processos, a redução da burocracia e a agilidade na tramitação de documentos proporcionada pelo *Blockchain* podem aumentar de maneira significativa a eficiência do sistema judiciário. Isso inclui a redução de etapas e a eliminação da necessidade de verificação manual de documentos, o que acelera a resolução dos processos e diminui o tempo de espera para os envolvidos¹⁷⁸.

Além disso, a otimização dos processos, a desmaterialização de documentos e a diminuição da necessidade de intermediários podem resultar em considerável economia de recursos. Menos uso de papel, menos etapas

¹⁷⁵ Hewa, T., Ylianttila, M. and Liyanage, M. (2021), “**Survey on blockchain based smart contracts: applications, opportunities and challenges**”, Journal of Network and Computer Applications, Vol. 177, doi: 10.1016/j.jnca.2020.102857.

¹⁷⁶ Estevam, G., Palma, L.M., Silva, L.R., Martina, J.E. and Vigil, M. (2021), “**Accurate and decentralized timestamping using smart contracts on the ethereum blockchain**”, Information Processing and Management, Vol. 58 No. 3, 102471, doi: 10.1016/j.ipm.2020.102471.

¹⁷⁷ Di Sorbo, A., Laudanna, S., Vacca, A., Visaggio, C.A. and Canfora, G. (2022), “**Profiling gas consumption in solidity smart contracts**”, Journal of Systems and Software, Vol. 186, 111193, doi: 10.1016/j.jss.2021.111193.

¹⁷⁸ Hewa, T., Ylianttila, M. and Liyanage, M. (2021), “**Survey on blockchain based smart contracts: applications, opportunities and challenges**”, Journal of Network and Computer Applications, Vol. 177, doi: 10.1016/j.jnca.2020.102857.

intermediárias e mais processos automatizados significam uma redução drástica dos custos operacionais para o Judiciário¹⁷⁹.

O ponto anunciado anteriormente, mas que ocupa o palco principal se resume na garantia da segurança e a imutabilidade dos dados, protegendo contra fraudes, adulterações e acessos indevidos. Cada registro na *Blockchain* é protegido por criptografia e distribuído por uma rede de nós, tornando extremamente difícil qualquer tipo de comprometimento ou ataque aos dados, assegurando a confiança em cada etapa do processo judicial¹⁸⁰.

2.2.4 Serviços de Tradução de Provas Estrangeiras

Com o avanço da globalização, os países estão se tornando cada vez mais interconectados, e o crescente número de casos com elementos estrangeiros tem aumentado a demanda por serviços especializados de tradução judicial.

Isto porque, em litígios judicializados envolvendo elementos estrangeiros, diversos tipos de documentos, na maioria das situações, devem ser traduzidos em conformidade com as leis das respectivas jurisdições, tal situação inclui decisões judiciais, registros, formulários e provas, com o intuito de garantir a proteção dos direitos e interesses legítimos das partes envolvidas¹⁸¹.

Em muitos países ou regiões, a tradução de documentos judiciais, como certificações, provas e petições, que devem ser apresentados aos tribunais nacionais, assim como documentos importantes para algumas empresas, como contratos e patentes, não são realizadas por tradutores ligados ao sistema judiciário¹⁸².

¹⁷⁹ Casino, F., Dasaklis, T.K. and Patsakis, C. (2019), “**A systematic literature review of blockchain-based applications: current status, classification and open issues**”, *Telematics and Informatics*, Vol. 36, pp. 55-81, doi: 10.1016/j.tele.2018.11.006.

¹⁸⁰ Belchior, R., Correia, M. and Vasconcelos, A. (2019), “**Justicechain: using blockchain to protect justice logs**”, *Lecture Notes in Computer Science*, Vol. 11877, pp. 318-325, doi: 10.1007/978-3-030-33246-4_21.

¹⁸¹ Farrokhi, M. (2019), “**The role of legal translation in the interpretation of international law documents**”, *Russian Law Journal*, Vol. 7 No. 1, pp. 55-86, doi: 10.17589/2309-8678-2019-7-1-55-86.

¹⁸² Scott, J. (2019), “**Specifying levels of (C)overtness in legal translation briefs**”, *Legal Translation. Current Issues and Challenges in Research, Methods and Applications*, pp. 243-262.

Além disso, em certos casos, documentos como decisões, intimações e ordens judiciais, destinados a partes que falam outro idioma, são transferidos pelos cartórios judiciais, via servidores, para empresas ou tradutores que fazem parte de listas do tribunal, ou diretamente terceirizados para empresas especializadas em tradução¹⁸³.

Durante esse processo, a transferência dos documentos por diferentes meios aumenta, sem dúvida, o risco de vazamentos, alterações e distorção de informações.

Neste contexto, o *blockchain* se resume em uma tecnologia de banco de dados descentralizada e distribuída, que possibilita a comunicação de dados por meio de protocolos de rede P2P, utilizando técnicas de criptografia para formar blocos de dados validados por vários nós que participam da confirmação das informações de transação¹⁸⁴. O armazenamento descentralizado e distribuído torna os dados mais abertos e transparentes, enquanto o uso de sequências de blocos e carimbos de data/hora assegura que os dados sejam rastreáveis e difíceis de falsificar¹⁸⁵.

Na prática judicial, a transferência segura e o armazenamento de documentos relacionados a casos que necessitam de tradução é uma parte essencial do processo de julgamento de litígios internacionais.

Em primeiro lugar, no que tange aos tradutores e empresas de tradução, a ética profissional é uma diretriz fundamental, visto que tradutores freelancers ou empresas de tradução precisam assinar acordos de confidencialidade com seus clientes ao assumir projetos que envolvem documentos sigilosos, mas ainda assim vazamentos de informações não são incomuns¹⁸⁶.

¹⁸³ Scott, J. (2019), “**Specifying levels of (C)overtness in legal translation briefs**”, *Legal Translation. Current Issues and Challenges in Research, Methods and Applications*, pp. 243-262.

¹⁸⁴ Huang, Lingling. Zhao, Chengquiang. Chen, Shijie. Zeng, Liujing. **Blockchain: a promising technology for judicial translation services in cases with foreign elements**. *Aslib Journal Information Management*. Vol. 76 No. 5, 2024. Pp. 713-735. DOI 10.1108/AJIM-11-2022-0485.

¹⁸⁵ Nakamoto, S. (2008), “**Bitcoin: a peer-to-peer electronic cash system**”. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acessado em mai. 2024.

¹⁸⁶ Huang, Lingling. Zhao, Chengquiang. Chen, Shijie. Zeng, Liujing. **Blockchain: a promising technology for judicial translation services in cases with foreign elements**. *Aslib Journal Information Management*. Vol. 76 No. 5, 2024. Pp. 713-735. DOI 10.1108/AJIM-11-2022-0485.

A título de exemplo, segundo o Japan Times, a Agência de Regulação Nuclear (NRA) do Japão relatou que uma empresa de tradução violou acordos de confidencialidade ao vazar informações sobre como “o combustível nuclear é reprocessado”, além de regulamentos e detalhes sobre usinas nucleares, o que quase resultou em uma grave crise de relações públicas para o governo japonês¹⁸⁷.

Em segundo lugar, quanto à transferência e armazenamento de dados por redes das quais apresentam vulnerabilidades e suportam ataques de

Exemplo disso é o caso da Interpreters Unlimited, uma empresa sediada na Califórnia, que prestava serviços a grandes empresas de tecnologia, como Google e Boeing, e sofreu um grande vazamento de dados devido a uma unidade de backup desprotegida, comprometendo informações pessoais e corporativas, incluindo registros judiciais¹⁸⁸.

Ademais, algumas empresas de tradução, tradutores ou advogados bilíngues podem recorrer a ferramentas de tradução automática, e há indícios de que tribunais podem recorrer diretamente ao Google Translate em situações de barreira linguística, o que representa um risco para a segurança dos dados¹⁸⁹.

Um exemplo ilustrativo é o caso da Statoil (atualmente conhecida como Equinor), uma das maiores empresas de energia do mundo, que utilizou o site translate.com, uma ferramenta gratuita de tradução online, durante uma transação de negócios de 46 bilhões de dólares, envolvendo a tradução de informações sensíveis como demissões, terceirizações, senhas, códigos e contratos¹⁹⁰.

¹⁸⁷ The Japan Times (2015), “**Translation firm leaked classified document, NRA says**”, Disponível em: <https://www.japantimes.co.jp/news/2015/04/01/national/translation-firm-leaked-classified-nrdocument-onto-internet-secretariat/>. Acesso em 20 Mai. 2024.

¹⁸⁸ Ashok, I. (2017), “**Silicon Valley translation firm with Google, Boeing and other clients hit with data leak**”, International Business Times UK, Disponível em: <https://www.ibtimes.co.uk/silicon-valleytranslation-firm-google-boeing-other-clients-hit-data-leak-1602177> Acesso em 20 Mai. 2024.

¹⁸⁹ Scott, J. and O'Shea, J. (2021), “**How legal documents translated outside institutions affect lives, businesses and the economy**”, International Journal for the Semiotics of Law - Revue Internationale De Semiotique Juridique, Vol. 34 No. 5, pp. 1331-1373, doi: 10.1007/s11196-020-09815-5.

¹⁹⁰ Tomter, L., Zondag, M.H.W. and Skille, Ø.B. (2017), “**Warning about translation web site: passwords and contracts accessible on the internet. NRK**”, Disponível em: https://www.nrk.no/urix/warningabout-translation-web-site_-passwords-and-contracts-accessible-on-the-internet-1.13670874. Acesso em 20 Mai. 2024.

Isso demonstra que documentos que exigem tradução podem ser facilmente vazados por vários canais, tornando imperativa a implementação de medidas de supervisão e proteção de segurança ao longo de todo o processo de transferência, tradução e armazenamento desses documentos.

Com base nisso, a fim de aprimorar a qualidade e a eficiência dos serviços de tradução envolvidos em litígios, um programa descentralizado baseado em *blockchain* indica a possibilidade de garantir, de maneira eficaz, a segurança e a privacidade na transferência e armazenamento de documentos judiciais em casos internacionais, além de possibilitar a credibilidade e a rastreabilidade do feedback e da avaliação dos serviços de tradução judicial.

2.2.5 Depósito Eletrônico de Dados de Direitos Autorais

A abordagem de direitos autorais digitais está diretamente vinculada ao avanço da tecnologia, cujo modelo de funcionamento, caracterizado pela facilidade de cópia, distribuição e pela operação de forma não linear, impôs novos desafios à proteção desses direitos¹⁹¹.

A tecnologia *blockchain* oferece uma solução ao registrar dados eletrônicos em blocos, abordando as dificuldades de rastreabilidade e a limitada credibilidade na autenticação de direitos autorais digitais.

Utilizando certificados de armazenamento eletrônico de dados em *blockchain*, assegura-se a integridade dos direitos autorais digitais. Por meio de carimbos de tempo confiáveis, assinaturas eletrônicas, hashing e outras tecnologias, garante-se que os dados eletrônicos permaneçam inalterados, para garantir a segurança desses dados, o certificado de depósito eletrônico em *blockchain* possui um controle rigoroso de temporalidade e, devido à irreversibilidade dos registros

¹⁹¹ D. Yang, ***Blockchain has the law***, China Renmin University Press, 2018.

temporais na *blockchain*, é possível assegurar a credibilidade do momento de depósito¹⁹².

Em junho de 2018, o Tribunal da Internet de Hangzhou proferiu uma decisão em um caso de violação dos direitos de disseminação de obras em rede, reconhecendo pela primeira vez a validade legal de dados eletrônicos depositados com o uso de tecnologia *blockchain*¹⁹³.

Na decisão do Tribunal da Internet de Hangzhou, a corte considerou que a plataforma de armazenamento de evidências de terceiros foi implementada no servidor geral da Alibaba Cloud e foi reconhecida pela indústria devido à certificação de segurança de primeiro nível do site. Salvo a apresentação de evidências em contrário, o site deve ser considerado como um ambiente seguro para a geração de dados eletrônicos. Do ponto de vista técnico, os programas puppeteer e curl são automaticamente acionados pela plataforma de armazenamento de terceiros para realizar a extração de páginas web e a identificação do código-fonte dos links-alvo. Esses processos são abertos e universais, e uma série de operações são automaticamente executadas pelo computador conforme procedimentos predefinidos¹⁹⁴.

À vista disso, considerando a existência de precedentes judiciais internacionais, o uso da tecnologia *blockchain* também se verifica eficaz na proteção de direitos autorais.

¹⁹² Zheng, Deyuan. **Reserach on the Judicial Application of Copyright in *Blockchain* Electronic Deposit**. Advances in Social Science, Education and Humanities Research, volume 517 Proceedings of the 6th Annual International Conference on Social Science and Contemporary Humanity Development (SSCHD 2020).

¹⁹³ The Supreme People's Court, **The Supreme People's Court promulgated the Internet court regulations, China Information Security**, 2018, pp. 9:30-33.

¹⁹⁴ Zheng, Deyuan. **Reserach on the Judicial Application of Copyright in *Blockchain* Electronic Deposit**. Advances in Social Science, Education and Humanities Research, volume 517 Proceedings of the 6th Annual International Conference on Social Science and Contemporary Humanity Development (SSCHD 2020).

2.3 DESAFIOS ESPERADOS

A adoção da tecnologia *Blockchain* no âmbito do Judiciário apresenta uma série de desafios que necessitam ser meticulosamente avaliados e considerados de maneira detalhada.

2.3.1 Legislação

Em um primeiro ponto, enfrenta-se o “Dilema de Collingridge”, o qual ressalta a complexidade de regular tecnologias emergentes como o *blockchain*. Ele destaca um problema crítico de tempestividade: intervir muito cedo pode sufocar a inovação, enquanto agir tarde demais pode levar a consequências sociais potencialmente irreversíveis¹⁹⁵.

Além disso, legislação vigente pode não estar plenamente adaptada à aplicação da *Blockchain*, fazendo-se necessária uma atualização normativa, que assegure a validade jurídica dos atos formalizados nesta tecnologia. Esta atualização pode exigir um processo longo e detalhado de revisão de leis e regulamentos para garantir que todos os aspectos jurídicos sejam considerados¹⁹⁶.

A legislação brasileira carece de um arcabouço jurídico específico para a *Blockchain*, gerando incertezas e desafios para sua implementação no setor judicial. Estes desafios regulatórios devem ser abordados para promover uma integração segura e legal da tecnologia.

Nesse sentido, a legislação deve ser revisada e atualizada para reconhecer a validade jurídica dos registros efetuados em *Blockchain*, assegurando que tais registros possam ser utilizados de forma legal e efetiva¹⁹⁷.

¹⁹⁵ Collingridge, D. (1980). **The social control of technology**. New York: St. Martin's Press.

¹⁹⁶ ROBICHEZ, G. et al. **Blockchain para governos e serviços públicos**. Rio de Janeiro: PUC, 2019. Disponível em: https://www.researchgate.net/profile/Paulo-Henrique-Alves-2/publication/331651536_Blockchain_para_Governo_e_Servicos_Publicos/links/5c86e704458515b59e452f93/Blockchain-paraGoverno-e-Servicos-Publicos.pdf. Acesso em: 16 mai. 2024.

¹⁹⁷ ENCCLA. **Blockchain no setor público: guia de conceitos e usos potenciais**. [Brasília, DF], 2020. Disponível em: <http://enccla.camara.leg.br/acoes/arquivos/resultados-enccla-2020/blockchainno-setor-publico-guia-de-conceitos-e-usos-potenciais/view>. Acesso em: 22 maio 2024.

Deve-se garantir que os registros em *Blockchain* possuam validade jurídica e sejam aceitos como provas em processos judiciais, assegurando que as evidências digitais sejam reconhecidas¹⁹⁸.

Igualmente, imperioso definir claramente as responsabilidades legais em caso de falhas ou incidentes relacionados à *Blockchain*, evitando ambiguidades e disputas jurídicas¹⁹⁹.

Tal fato auxiliaria na própria resistência à inovação inserida na atual cultura organizacional do Judiciário, caracterizada por um viés conservador, pode manifestar resistência significativa à incorporação de tecnologias emergentes. Essa resistência pode se manifestar de várias formas, incluindo a falta de compreensão dos benefícios da tecnologia, medo das mudanças necessárias e uma preferência pelos métodos tradicionais estabelecidos²⁰⁰.

Conforme aludido anteriormente, a implementação da *Blockchain* requer investimentos robustos em infraestrutura, desenvolvimento de novos sistemas e capacitação técnica dos profissionais envolvidos sobretudo no sistema de contratação de servidores públicos. Isto inclui a aquisição de hardware especializado, desenvolvimento de software compatível com a *Blockchain* e a realização de treinamentos para assegurar que os profissionais possam utilizar a nova tecnologia de maneira eficaz²⁰¹.

¹⁹⁸ ALCÂNTARA, L. T. et al. **Uso da tecnologia *Blockchain* como instrumento de governança eletrônica no setor público**. In: II CONGRESSO INTERNACIONAL DE CONTABILIDADE PÚBLICA, Lisboa, 2019. Anais [...]. Lisboa, PT, 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/34651/1/EVENTO_UsoTecnologiaBlockchain.pdf. Acesso em: 7 jun. 2024.

¹⁹⁹ ROBICHEZ, G. et al. ***Blockchain para governos e serviços públicos***. Rio de Janeiro: PUC, 2019. Disponível em: https://www.researchgate.net/profile/Paulo-Henrique-Alves-2/publication/331651536_Blockchain_para_Governo_e_Servicos_Publicos/links/5c86e704458515b59e452f93/Blockchain-paraGoverno-e-Servicos-Publicos.pdf. Acesso em: 16 mai. 2024.

²⁰⁰ GOMES, V. J. F.; UCHOA, S. B. B.; SANTOS, T. F. S. **Mapeamento tecnológico das patentes desenvolvidas a partir da tecnologia *Blockchain*: um cenário global**. Cadernos de Prospecção, Salvador, v. 11, n. 4, p. 1.166-1.181, dezembro, 2018. Disponível em: <https://periodicos.ufba.br/index.php/nit/article/view/27193>. Acesso em: 24 mai. 2024.

²⁰¹ FERREIRA, J. E.; PINTO, F. G. C.; DOS SANTOS, S. C. **Estudo de mapeamento sistemático sobre as tendências e desafios do *Blockchain***. Gestão. Org., [s.l.], v. 15, n. 6, p. 108-117, 2017. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/231244>. Acesso em: 19 mai. 2024.

2.3.2 Operação Técnica

Acerca da infraestrutura, é igualmente imprescindível assegurar a interoperabilidade entre os sistemas legados do Judiciário e a nova tecnologia *Blockchain*, de maneira que esta possa ser integrada eficientemente aos processos preexistentes. Garantir essa interoperabilidade pode ser um desafio técnico considerável, exigindo soluções de integração que permitam a comunicação eficaz entre diferentes tipos de sistemas e plataformas tecnológicas²⁰².

A integração da *Blockchain* com os sistemas legados do Judiciário acarreta desafios técnicos de elevada complexidade que precisam ser cuidadosamente considerados e resolvidos.

É crucial garantir a comunicação e a troca de dados entre a *Blockchain* e os sistemas preexistentes, muitos dos quais utilizam tecnologias obsoletas e formatos de dados incompatíveis. Este desafio técnico exige soluções inovadoras que permitam uma integração eficaz²⁰³.

Noutra seara, é necessário assegurar que a *Blockchain* possa suportar o alto volume de dados e transações inerentes ao Judiciário, sem comprometer o desempenho. Garantir a escalabilidade é essencial para a operação contínua de sistemas de grande porte²⁰⁴.

A seleção da plataforma *Blockchain* mais adequada às necessidades do Judiciário deve considerar fatores como segurança, escalabilidade, custo e funcionalidades específicas. A escolha correta da plataforma pode determinar o sucesso da implementação²⁰⁵.

²⁰² NAKAMOTO, S. **Bitcoin: a peer-to-peer electronic cash system**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 14 mai. 2024.

²⁰³ ROBICHEZ, G. et al. **Blockchain para governos e serviços públicos**. Rio de Janeiro: PUC, 2019. Disponível em: https://www.researchgate.net/profile/Paulo-Henrique-Alves-2/publication/331651536_Blockchain_para_Governo_e_Servicos_Publicos/links/5c86e704458515b59e452f93/Blockchain-paraGoverno-e-Servicos-Publicos.pdf. Acesso em: 16 mai. 2024.

²⁰⁴ FERREIRA, J. E.; PINTO, F. G. C.; DOS SANTOS, S. C. **Estudo de mapeamento sistemático sobre as tendências e desafios do Blockchain**. Gestão. Org., [s.l.], v. 15, n. 6, p. 108-117, 2017. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/231244>. Acesso em: 19 mai. 2024

²⁰⁵ ALCÂNTARA, L. T. et al. **Uso da tecnologia Blockchain como instrumento de governança eletrônica no setor público**. In: II CONGRESSO INTERNACIONAL DE CONTABILIDADE PÚBLICA,

Não bastassem tais pontos de relevância, importante destacar que o Judiciário, embora disponha de mecanismos de segurança avançados, permanece vulnerável a diversos tipos de incidentes que precisam ser cuidadosamente monitorados e mitigados, inclusive sob a ótica da utilização da *Blockchain*.

Em momento anterior à própria inclusão de documentos nos sistemas do PJSC a falsificação de documentos, manipulação de prazos e distorção de informações com o objetivo de obter indevidos benefícios se mostram um grande desafio²⁰⁶.

Noutro ponto, o vazamento de informações confidenciais, violação do sigilo profissional e acesso não autorizado a dados sensíveis continuam igualmente suscetíveis, haja vista que tal insegurança é mitigada por uma estratégia de gestão de acessos baseada em perfis com autorização baseada na função²⁰⁷.

Não se exime igualmente de ataques cibernéticos, os quais compreendem a invasão de sistemas, o roubo de dados, o sequestro de informações (ransomware) e a interrupção de serviços. Esses ataques representam uma ameaça constante e exigem medidas de segurança robustas e diversas para mitigar seus efeitos²⁰⁸.

Como base da utilização de tecnologia, os erros humanos também incluem-se como ponto de atenção, englobando falhas na manipulação de dados, perda de documentos e envio de informações para destinatários incorretos. Apesar da melhor tecnologia, os erros humanos permanecem uma fonte comum de incidentes que podem comprometer a eficiência e a segurança²⁰⁹.

Lisboa, 2019. Anais [...]. Lisboa, PT, 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/34651/1/EVENTO_UsoTecnologiaBlockchain.pdf. Acesso em: 7 jun. 2024.

²⁰⁶ Ching, J. (2016). **Is blockchain evidence inadmissible hearsay?** Disponível em: <https://www.law.com/sites/almstaff/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/>. Acesso em 19 mai. 2024.

²⁰⁷ Ching, J. (2016). **Is blockchain evidence inadmissible hearsay?** Disponível em: <https://www.law.com/sites/almstaff/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/>. Acesso em 19 mai. 2024.

²⁰⁸ Hileman, G., and Rauchs, M. (2017). **global blockchain benchmarking study**. SSRN Electron. J., doi:10.2139/ssrn.3040224. 2017

²⁰⁹ Glendon, M. A., Carozza, P. G., and Picker, C. B. **Comparative legal traditions in a nutshell**. St. Paul, MN: West Academic Publishing. 2016

2.3.3 Cultura Organizacional

A cultura organizacional predominantemente conservadora do Judiciário pode representar um obstáculo significativo à implementação da *Blockchain*. Para superar esses desafios, uma mudança cultural e organizacional se mostra essencial, fato curiosamente coincidente durante a implementação da digitalização de processos físicos, fato histórico em relação à revolução de tramitação de processos.

Fato é que, magistrados, servidores e operadores do direito podem resistir à adoção de novas tecnologias por falta de conhecimento, receio de mudanças ou apego a métodos tradicionais. Superar essa resistência é crucial para a implementação bem-sucedida²¹⁰.

Além disso, a utilização da *Blockchain* exige um processo de treinamento e capacitação para que os usuários possam utilizá-la de maneira eficiente e segura. Programas de educação específicos e contínuos são necessários para minimizar a resistência e maximizar o uso eficaz da tecnologia²¹¹.

Por fim, talvez o maior desafio presente na operabilidade de tais sistemas recai sob a possibilidade de exigir revisões e adaptações de processos existentes, o que pode gerar resistência e dificuldades adicionais. Planejar e gerenciar essas mudanças de maneira eficaz é essencial para a adoção bem-sucedida da tecnologia²¹².

²¹⁰ Hileman, G., and Rauchs, M. **global blockchain benchmarking study**. SSRN Electron. J., doi:10.2139/ssrn.3040224. 2017.

²¹¹ ROBICHEZ, G. et al. **Blockchain para governos e serviços públicos**. Rio de Janeiro: PUC, 2019. Disponível em: https://www.researchgate.net/profile/Paulo-Henrique-Alves-2/publication/331651536_Blockchain_para_Governo_e_Servicos_Publicos/links/5c86e704458515b59e452f93/Blockchain-paraGoverno-e-Servicos-Publicos.pdf. Acesso em: 16 mai. 2024.

²¹² ROBICHEZ, G. et al. **Blockchain para governos e serviços públicos**. Rio de Janeiro: PUC, 2019. Disponível em: https://www.researchgate.net/profile/Paulo-Henrique-Alves-2/publication/331651536_Blockchain_para_Governo_e_Servicos_Publicos/links/5c86e704458515b59e452f93/Blockchain-paraGoverno-e-Servicos-Publicos.pdf. Acesso em: 16 mai. 2024.

2.3.4 Investimento

A implementação da *Blockchain* no Judiciário demanda investimentos significativos em infraestrutura, desenvolvimento de sistemas e capacitação pessoal.

Tanto o programa de compliance digital quanto ferramentas de segurança de informação se resumem em medidas preventivas, ou seja, as organizações públicas e privadas na maioria dos casos não observam a redução indireta de custos obtida em benefício à utilização e implementação dos mesmos.

Em situação exemplificativa e comparativa análoga, trata-se da mesma economia indireta obtida em favor do Estado na área da saúde quando devidamente implementados investimentos na área de saneamento básico de municípios.

Na situação em questão, a criação de uma plataforma *Blockchain* robusta e segura, integrada aos sistemas legados, requer investimentos substanciais em tecnologia e expertise especializada. Esses investimentos são cruciais para garantir a confiabilidade e segurança da nova tecnologia²¹³.

Não bastando apenas implementar, a *Blockchain* exige custos contínuos de manutenção, atualização e suporte técnico. Esses custos devem ser considerados no planejamento orçamentário de longo prazo para garantir a sustentabilidade da tecnologia²¹⁴.

Conforme aludido acima, é fundamental avaliar o retorno sobre o investimento em *Blockchain*, considerando os benefícios em termos de eficiência, segurança e redução de custos a longo prazo. Medir e monitorar esses benefícios ao longo do tempo ajudará a justificar os investimentos iniciais e contínuos²¹⁵.

²¹³ FERREIRA, J. E.; PINTO, F. G. C.; DOS SANTOS, S. C. **Estudo de mapeamento sistemático sobre as tendências e desafios do *Blockchain***. Gestão. Org., [s.l.], v. 15, n. 6, p. 108-117, 2017. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/231244>. Acesso em: 19 mai. 2024

²¹⁴ FREITAS, Juarez; TEIXEIRA, Anderson Vichinkeski. **Democracia digital e avaliação continuada de políticas públicas**. Revista Brasileira de Estudos Políticos. Belo Horizonte, n. 119, pp. 227-252, jul./dez. 2019. Disponível em: <https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/715>. Acesso em: 22 jun. 2024.

²¹⁵ GREMBERGEN, Wim van; DE HAES, Steven. **Implementing Information Technology Governance: models, practices, and cases**. IGI Publishing, 2008.

Capítulo 3

ANALISANDO TRIBUNAIS NACIONAIS E INTERNACIONAIS

3.1 IMPLEMENTAÇÕES DE *BLOCKCHAIN* NO JUDICIÁRIO BRASILEIRO

A *Blockchain*, apesar de ser uma tecnologia relativamente nova, está sendo utilizada em projetos piloto e iniciativas inovadoras no Judiciário em diversos países. Os estudos de caso a seguir ilustram o potencial da *Blockchain* para a construção de um sistema mais eficiente, transparente e seguro.

3.1.1 Tribunal de Contas da União

Na qualidade de um destaque nacional, o Tribunal de Contas da União (TCU), em parceria com o Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e com a Rede *Blockchain* Brasil se encontram em fase piloto no intuito de implementar e desenvolver a infraestrutura de um ambiente de nós formulado com base na *blockchain* em prol do governo²¹⁶.

Ainda que a parceria tenha sido iniciada pelo TCU e o BNDES por meio de acordo de cooperação técnica, diversas instituições aderiram ao programa, a exemplo da Empresa de Tecnologia e Informações da Previdência (Dataprev), o Serviço Federal de Processamento de Dados (Serpro), a Companhia de Tecnologia da Informação do Estado de Minas Gerais (Prodemge) e a Secretaria de Estado de Transparência e Controle do governo do Maranhão²¹⁷.

O Secretário de Tecnologia da Informação e Evolução Digital do TCU destacou que a rede poderá ser utilizada para gerenciar dados sensíveis e identidades

²¹⁶ TCU. **Rede *Blockchain* Brasil Inicia Fase Piloto do Projeto**. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/rede-blockchain-brasil-inicia-fase-piloto-do-projeto.htm>

²¹⁷ TCU. **Rede *Blockchain* Brasil Inicia Fase Piloto do Projeto**. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/rede-blockchain-brasil-inicia-fase-piloto-do-projeto.htm>

digitais descentralizadas, bem como oportunizar privacidade e segurança aos usuários, ademais, destacou futuras aplicações em áreas como saúde, educação e segurança pública²¹⁸.

Muito embora se trate de um projeto que se encontra em fase piloto no ano corrente da presente dissertação, sem dúvidas se trata de um dos pioneiros na história de tribunais brasileiros que fornecerá estrutura aos demais tribunais.

3.1.2 Tribunal de Justiça do Maranhão

O Tribunal de Justiça do Estado do Maranhão (TJMA) iniciou a adoção da tecnologia *blockchain* como parte de um projeto piloto voltado para a autenticação e armazenamento seguro de documentos processuais²¹⁹.

A principal motivação foi garantir a integridade e a imutabilidade das informações judiciais²²⁰.

O TJMA utilizou uma plataforma “*blockchain* permissionada”, permitindo que apenas participantes autorizados adicionassem registros, além disso, um sistema de auditoria contínua foi implementado para monitorar o uso e eficácia da tecnologia²²¹.

Entre os desafios destacados, estavam a resistência inicial dos servidores e a adaptação dos sistemas legados à nova tecnologia. Para superar esses obstáculos, foram realizados treinamentos e workshops para capacitar servidores e magistrados²²².

²¹⁸ TCU. **Rede *Blockchain* Brasil Inicia Fase Piloto do Projeto**. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/rede-blockchain-brasil-inicia-fase-piloto-do-projeto.htm>

²¹⁹ EXAME. **Maranhão é o primeiro estado do país a aderir à Rede *Blockchain* Brasil**. *Exame*, São Paulo, 8 ago. 2023. Disponível em: <https://exame.com/future-of-money/maranhao-primeiro-estado-rede-blockchain-brasil/>. Acesso em: 14 out. 2024.

²²⁰ EXAME. **Maranhão é o primeiro estado do país a aderir à Rede *Blockchain* Brasil**. *Exame*, São Paulo, 8 ago. 2023. Disponível em: <https://exame.com/future-of-money/maranhao-primeiro-estado-rede-blockchain-brasil/>. Acesso em: 14 out. 2024.

²²¹ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **MA: Centro de Inteligência do Judiciário discute projetos de tecnologia e inovação**. CNJ, 30 dez. 2021. Disponível em: <https://www.cnj.jus.br/ma-centro-de-inteligencia-do-judiciario-discute-projetos-de-tecnologia-e-inovacao/>. Acesso em: 14 out. 2024.

²²² CONSELHO NACIONAL DE JUSTIÇA (CNJ). **MA: Centro de Inteligência do Judiciário discute projetos de tecnologia e inovação**. CNJ, 30 dez. 2021. Disponível em: <https://www.cnj.jus.br/ma-centro-de-inteligencia-do-judiciario-discute-projetos-de-tecnologia-e-inovacao/>

Transpassados os desafios, verificou-se que a adoção da tecnologia resultou em um aumento significativo na segurança documental e na confiabilidade dos registros processuais.

3.1.3 Tribunal de Justiça do Rio Grande do Sul

Por meio do Provimento nº 38/2021, a Corregedoria Geral da Justiça em parceria com TJRS regulamentou a lavratura de escrituras públicas de permuta de imóveis com contrapartida de tokens/criptoativos, assim como o registro imobiliário da operação, constituindo um marco normativo no processo de modernização e aperfeiçoamento dos serviços notariais e de registro no âmbito estadual. Este ato normativo objetiva promover a padronização de procedimentos administrativos e o incremento da segurança jurídica, com foco na digitalização e na otimização das atividades cartorárias²²³.

A normativa reflete a crescente necessidade de adequação dos serviços extrajudiciais às demandas tecnológicas contemporâneas, proporcionando uma maior eficiência, transparência e acessibilidade aos usuários. Entre as principais inovações introduzidas, destaca-se a implementação de mecanismos eletrônicos para a realização de atos notariais e registrais, alinhando-se às diretrizes nacionais que incentivam a desburocratização e a digitalização de processos²²⁴.

Além disso, o provimento estabelece medidas de fiscalização e orientação por parte da Corregedoria, visando garantir o cumprimento das novas

centro-de-inteligencia-do-judiciario-discute-projetos-de-tecnologia-e-inovacao/. Acesso em: 14 out. 2024.

²²³ TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. **CGJ regulamenta escritura pública de imóveis por token/criptoativo**. Disponível em: <https://www.tjrs.jus.br/novo/noticia/cgj-regulamenta-escritura-publica-de-imoveis-por-token-criptoativo/>. Acesso em: 20 out. 2024.

²²⁴ TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. **CGJ regulamenta escritura pública de imóveis por token/criptoativo**. Disponível em: <https://www.tjrs.jus.br/novo/noticia/cgj-regulamenta-escritura-publica-de-imoveis-por-token-criptoativo/>. Acesso em: 20 out. 2024.

normas e assegurar a conformidade com os princípios de publicidade, autenticidade e segurança²²⁵.

Assim, o Provimento nº 038/2021 se configura como uma resposta institucional ao avanço das tecnologias da informação no setor jurídico, promovendo uma reestruturação organizacional que visa atender, de maneira mais eficaz, as exigências da sociedade contemporânea²²⁶.

3.1.4 Conselho Nacional de Justiça

O Conselho Nacional de Justiça celebrou junto à Associação Brasileira de Criptoeconomia (ABCRIPTO) o Acordo de Cooperação Técnica nº 133/2024, o qual surge como uma iniciativa inovadora para promover a comunicação eletrônica entre o Judiciário e as Prestadoras de Serviços de Ativos Virtuais (PSAVs), facilitando a tramitação de ordens judiciais e a gestão de ativos digitais.

O acordo abrange diversos objetivos estratégicos, sendo o primeiro deles o desenvolvimento de ações educacionais conjuntas. Por meio dessa cooperação, CNJ e ABCRIPTO visam promover cursos, workshops, materiais informativos e pesquisas que capacitem tanto os operadores do direito quanto os profissionais do mercado financeiro digital. A disseminação do conhecimento sobre criptoativos, criptomoedas e tecnologias subjacentes, como *blockchain* e distributed ledger technologies (DLTs), é um dos pilares centrais dessa parceria²²⁷.

²²⁵ RIO GRANDE DO SUL (Estado). Tribunal de Justiça. Provimento nº 038/2021 - CGJ. **Regulamenta a lavratura de escrituras públicas de permuta de bens imóveis com contrapartida de tokens/criptoativos e o respectivo registro imobiliário pelos Serviços Notariais e de Registro do Rio Grande do Sul.** Porto Alegre: TJRS, 2021. Disponível em: <https://www.tjrs.jus.br/static/2021/11/Provimento-038-2021-CGJ.pdf>. Acesso em: 20 de out. 2024.

²²⁶ RIO GRANDE DO SUL (Estado). Tribunal de Justiça. Provimento nº 038/2021 - CGJ. **Regulamenta a lavratura de escrituras públicas de permuta de bens imóveis com contrapartida de tokens/criptoativos e o respectivo registro imobiliário pelos Serviços Notariais e de Registro do Rio Grande do Sul.** Porto Alegre: TJRS, 2021. Disponível em: <https://www.tjrs.jus.br/static/2021/11/Provimento-038-2021-CGJ.pdf>. Acesso em: 20 de out. 2024.

²²⁷ CONSELHO NACIONAL DE JUSTIÇA. **Acordo de Cooperação Técnica n.º 133/2024, celebrado entre o Conselho Nacional de Justiça e a Associação Brasileira de Criptoeconomia.** Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0. Acesso em: 20 out. 2024.

Outro ponto de destaque do acordo é o aperfeiçoamento da integração eletrônica entre o Poder Judiciário e as PSAVs. Nesse aspecto, o acordo estabelece a criação de um sistema digital, denominado Sistema Brasileiro de Interligação do Mercado de Criptomoedas, Criptoativos e Ativos Digitais ao Poder Judiciário, que tem como principal finalidade facilitar o envio e recebimento de ordens judiciais eletrônicas relacionadas a criptoativos. Tal sistema permitirá uma comunicação mais ágil entre o Judiciário e as prestadoras de serviços do mercado de criptoeconomia, garantindo uma tramitação processual mais célere e eficiente. Essa integração tecnológica é essencial para acompanhar a crescente complexidade das operações financeiras digitais e as demandas do Judiciário por informações rápidas e precisas²²⁸.

Além disso, o acordo prevê o desenvolvimento e implementação de sistemas de custódia e liquidação de criptoativos. Esses sistemas eletrônicos serão responsáveis por gerir criptoativos constrictos em processos judiciais, garantindo a segurança e a integridade das operações. Com o aumento do uso de criptoativos em transações globais e o consequente envolvimento desses ativos em disputas judiciais, torna-se indispensável a criação de ferramentas que assegurem o correto manejo desses bens digitais. Nesse sentido, o acordo não apenas facilita a tramitação processual, mas também reforça as estruturas de custódia e liquidação, elementos cruciais para a segurança jurídica²²⁹.

Em síntese, o Acordo de Cooperação Técnica nº 133/2024 é um exemplo concreto de como o Poder Judiciário pode se adaptar às inovações tecnológicas, integrando o mercado de criptoativos às suas práticas processuais e promovendo a segurança jurídica em um cenário digital cada vez mais complexo. A parceria entre CNJ e ABCRIPTO destaca-se como uma iniciativa pioneira, que busca não apenas otimizar a tramitação de ordens judiciais, mas também assegurar a

²²⁸ CONSELHO NACIONAL DE JUSTIÇA. **Acordo de Cooperação Técnica n.º 133/2024, celebrado entre o Conselho Nacional de Justiça e a Associação Brasileira de Criptoeconomia**. Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0. Acesso em: 20 out. 2024.

²²⁹ CONSELHO NACIONAL DE JUSTIÇA. **Acordo de Cooperação Técnica n.º 133/2024, celebrado entre o Conselho Nacional de Justiça e a Associação Brasileira de Criptoeconomia**. Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0. Acesso em: 20 out. 2024.

segurança e integridade das informações e promover a disseminação do conhecimento sobre criptoeconomia²³⁰.

3.2 INICIATIVAS DA TECNOLOGIA *BLOCKCHAIN* EM OUTROS PAÍSES

Pesquisas recentes destacam o potencial da *blockchain* para transformar sistemas judiciais ao redor do mundo. Sob o viés da doutrina internacional, de acordo com Nakamoto²³¹, a estrutura descentralizada e segura da *blockchain* pode virtualmente eliminar fraudes documentais. Outro estudo realizado por Tapscott e Tapscott²³² enfatiza a capacidade da *blockchain* de trazer maior transparência aos registros judiciais, assegurando que todos os documentos permaneçam imutáveis. Esses estudos estabelecem um quadro teórico que justifica a exploração de casos práticos de implementação da tecnologia no Judiciário mundial.

3.2.1 África do Sul

Em 2013, aproximadamente 90% das terras situadas em áreas rurais da África do Sul encontravam-se indocumentadas ou não registradas, o que as torna altamente suscetíveis à apropriação indevida e à expropriação com compensações inadequadas²³³.

Nesse contexto, o primeiro registro de propriedade baseado em tecnologia *blockchain* foi implementado na África do Sul. Em 2019, a organização sem fins lucrativos Centre for Affordable Housing Finance Africa (CAHF), em colaboração com a consultoria de pesquisa estratégica “71point4” e a plataforma digital de

²³⁰ CONSELHO NACIONAL DE JUSTIÇA. **Acordo de Cooperação Técnica n.º 133/2024, celebrado entre o Conselho Nacional de Justiça e a Associação Brasileira de Criptoconomia**. Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0. Acesso em: 20 out. 2024.

²³¹ NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 10 maio 2024.

²³² TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**. Penguin, 2016.

²³³ World Bank. 2013. **How Africa Can Transform Land Tenure, Revolutionize Agriculture, and End Poverty**. Disponível em: <https://www.worldbank.org/en/news/press-release/2013/07/22/howafrica-can-transform-land-tenure-revolutionize-agriculture-end-poverty>. Acesso em: 20 out. 2024.

transações fundiárias “Seso Global”, desenvolveram um projeto inovador com o objetivo de registrar propriedades por meio da tecnologia *blockchain*²³⁴.

O projeto-piloto abrangeu uma área composta por cerca de 1.000 propriedades localizadas em quatro regiões de Makhaza, Khayelitsha. Todas as habitações incluídas no projeto consistiam em propriedades subsidiadas pelo governo que, até então, não haviam sido registradas no Deeds Registry²³⁵.

Além da África do Sul, em 2015, Gana implementou um projeto de registro digital de terras baseado em tecnologia *blockchain*, conduzido pela organização não governamental Bitland. O objetivo dessa iniciativa é proporcionar aos cidadãos, empresas e sindicatos agrícolas a capacidade de registrar formalmente suas propriedades e acessar um sistema de registro fundiário mais robusto, protegido pela tecnologia *blockchain*, o que confere maior transparência e segurança, tornando-o praticamente impossível de ser adulterado²³⁶.

A Bitland atua em parceria com a Comissão de Terras de Gana, realizando pesquisas de campo para confirmar a validade dos títulos de propriedade e registrando as coordenadas geográficas das propriedades no sistema digital. Além disso, a organização emite um certificado em papel para os proprietários, beneficiando especialmente aqueles que, por não possuírem documentação oficial, encontram-se à margem da proteção legal de suas propriedades²³⁷.

Esse banco de dados digital, protegido pela tecnologia *blockchain*, possui o potencial de facilitar a resolução de disputas fundiárias, uma vez que os certificados emitidos pela Bitland serviriam como referência confiável para a validação de direitos de propriedade²³⁸.

²³⁴ CAHF. 2020. **Exploring Technology in Residential Property Markets**. Centre for Affordable Housing Finance Africa.

²³⁵ CAHF. 2020. **Exploring Technology in Residential Property Markets**. Centre for Affordable Housing Finance Africa.

²³⁶ Miller, M. 2020. **Bitland: Property Rights for The World’s Poor. The Borgen Project**. Disponível em: <https://borgenproject.org/property-rights-for-the-worlds-poor/>. Acesso em 20 de Out. 2024.

²³⁷ Do4Africa. **Project Description**. Disponível em: <https://www.do4africa.org/en/projets/bitland-2/>. Acesso em 20 de Out. 2024.

²³⁸ Do4Africa. **Project Description**. Disponível em: <https://www.do4africa.org/en/projets/bitland-2/>. Acesso em 20 de Out. 2024.

Na fase final, os títulos de propriedade e seus arquivos correspondentes são convertidos em tokens, os quais podem ser tanto negociados quanto rastreados digitalmente²³⁹.

3.2.2 Estônia

Em 2012, a Estônia tornou-se o primeiro país a adotar tecnologias distribuídas com o objetivo de assegurar que seus cidadãos tenham confiança plena nos dados governamentais. O país utiliza uma implementação permissionada de *blockchain* para garantir a integridade dos dados. Dessa forma, quando uma organização pública possui um ativo digital, ela pode utilizar o serviço baseado em *blockchain* para comprovar que uma informação não foi alterada após o momento de seu registro²⁴⁰.

A tecnologia que sustenta os sistemas estonianos é a infraestrutura de assinatura sem chave (Keyless Signature Infrastructure – KSI), que também é utilizada pela Organização do Tratado do Atlântico Norte (OTAN) e pelo Departamento de Defesa dos Estados Unidos (DoD). O KSI é um sistema distribuído que oferece serviços de timestamp e assinatura digital com suporte a servidor²⁴¹.

Embora o termo "keyless" sugira a ausência de chaves criptográficas na criação de assinaturas, estas continuam a ser necessárias para autenticação; porém, as assinaturas podem ser verificadas com segurança sem depender do sigilo contínuo das chaves²⁴².

Esse sistema permite que, posteriormente, um usuário consulte o KSI utilizando um valor hash. Isso gera uma espécie de assinatura que oferece prova

²³⁹ Miller, M. 2020. **Bitland: Property Rights for The World's Poor. The Borgen Project**. Disponível em: <https://borgenproject.org/property-rights-for-the-worlds-poor/>. Acesso em 20 de Out. 2024.

²⁴⁰ GOVERNO DA ESTÔNIA, (2018) **E-ESTONIA**. Disponível em: <https://e-estonia.com/>. Acesso em 20 de Out. 2024.

²⁴¹ COUTO, Militello Gabriel. **Educação e pensamento computacional: Estudo de caso sobre a E- Estônia**. Relatório final de pesquisa. PUCSP, São Paulo. 2016.

²⁴² GOVERNO DA ESTÔNIA, 2024. **Segurança Cibernética**. Disponível em: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>. Acesso em 20 de Out. 2024.

criptográfica de tempo (proof-of-time), assegurando a integridade do dado assinado e a atribuição de sua origem, ou seja, qual entidade gerou a assinatura. Dessa forma, qualquer cidadão pode acessar o sistema e verificar quem manipulou seus dados (por exemplo, se a polícia de trânsito consultou sua placa ou se um médico acessou seus registros médicos)²⁴³.

A mencionada solução baseada em *blockchain* foi projetada para garantir que todas as interações com os dados sejam registradas de forma segura e protegidas contra adulterações por agentes mal-intencionados.

3.2.3 Malta

O governo de Malta aprovou três projetos de lei (43, 44 e 45), intitulados "Lei de Arranjos e Serviços de Tecnologia Inovadora"²⁴⁴, "Lei de Ativos Financeiros Virtuais"²⁴⁵ e "Lei da Autoridade de Inovação Digital de Malta"²⁴⁶, respectivamente.

Essas iniciativas legislativas foram elaboradas com o objetivo de fornecer diretrizes ao governo maltês sobre como integrar de forma eficaz a tecnologia *blockchain*, visando consolidar o país como um centro internacional de negócios voltados para criptomoedas.

O Projeto de Lei nº 45, em particular, prevê a criação da Autoridade de Inovação Digital de Malta, cuja principal atribuição será promover e desenvolver a indústria de *blockchain* no território maltês²⁴⁷.

²⁴³ GOVERNO DA ESTÔNIA, 2024. **Segurança Cibernética**. Disponível em: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>. Acesso em 20 de Out. 2024.

²⁴⁴ GOVERNO DE MALTA. **Lei de Arranjos e Serviços de Tecnologia Inovadora**. Disponível em: <https://parlament.mt/media/94207/bill-43-innovative-technology-arrangements-and-services-bill.pdf>. Acesso em 20 de Out. 2024.

²⁴⁵ GOVERNO DE MALTA. **Lei de Ativos Financeiros Virtuais**. Disponível em: <https://parlament.mt/media/94209/bill-44-virtual-financial-assets-bill.pdf>. Acesso em 20 de Out. 2024.

²⁴⁶ GOVERNO DE MALTA. **Lei da Autoridade de Inovação Digital de Malta**. Disponível em: <https://parlament.mt/media/94210/bill-45-malta-digital-innovation-authority-bill.pdf>. Acesso em 20 de Out. 2024.

²⁴⁷ COINDESK. **Malta Passes Three Bills on Blockchain and Crypto Assets**. Disponível em: <https://www.coindesk.com/malta-passes-three-bills-on-blockchain-and-crypto-assets>. Acesso em 21 de Out. 2024.

Durante o evento intitulado '*Blockchain – O Novo Quadro Regulatório*', o Presidente da Câmara de Comércio, Empresa e Indústria de Malta, destacou que "o *blockchain* tem o potencial de estabelecer novas bases para os sistemas econômicos e sociais globais, em vez de ser uma força disruptiva para os modelos de negócios tradicionais", afirmou ainda que "o *blockchain* promete proporcionar às corporações maior eficiência nas cadeias globais de suprimentos, nas transações financeiras, no registro de ativos e nas redes sociais descentralizadas"²⁴⁸.

Com esta movimentação, o governo de Malta estabeleceu um arcabouço legislativo que criou um ambiente favorável para o desenvolvimento de startups de criptomoedas e *blockchain*.

Suas políticas atraíram grandes plataformas de intercâmbio de criptomoedas, posicionando o país como uma das jurisdições mais receptivas ao setor de criptomoedas no mundo.

O que outros governos viam como uma ameaça, Malta enxergou como uma oportunidade de desenvolvimento. O marco regulatório implementado pelo governo maltês abrange diversos atores e instituições do mercado, como comerciantes de criptomoedas, gestores de ativos e plataformas de troca.

3.2.4 Emirados Árabes Unidos (Dubai)

Como parte de seus esforços para incorporar as mais recentes tecnologias e práticas de inovação em nível global, a Dubai Future Foundation anunciou a criação do Global *Blockchain Council*, com o objetivo de explorar e discutir as aplicações atuais e futuras da tecnologia, além de promover a organização de transações por meio da plataforma *blockchain*²⁴⁹.

²⁴⁸ CÂMARA DE MALTA. ***Blockchain, The New Regulatory Framework***. Disponível em: <https://www.maltachamber.org.mt/en/blockchain-the-new-regulatory-framework>. Acesso em 21 de Out. 2024.

²⁴⁹ Dubai *Blockchain Policy*. **Dubai Future Council**. Disponível em: <https://www.digitaldubai.ae/docs/default-source/publications/reference-document--dubai-blockchain-policy.pdf?sfvrsn=19522b4>. Acesso em 20 de Out. 2024.

Em abril de 2018, o governo lançou a Dubai *Blockchain* Strategy 2021, com a finalidade de utilizar a tecnologia *blockchain* para transformar 50% das transações governamentais para essa plataforma até o ano de 2021²⁵⁰.

A estratégia está fundamentada em três pilares: eficiência governamental, incentivo à indústria e liderança tecnológica em âmbito internacional. O país pretende utilizar a tecnologia *blockchain* para realizar transações digitais, atribuindo a cada usuário um número de identificação exclusivo vinculado às suas informações na rede²⁵¹.

Ao adotar essa tecnologia, o governo dos Emirados Árabes Unidos espera otimizar recursos financeiros e temporais, eliminando a necessidade de transações e documentos atualmente processados em papel.

3.2.5 Estados Unidos da América

Nos Estados Unidos, várias iniciativas locais têm explorado a tecnologia *blockchain* no Judiciário. Um exemplo notável é o uso de *blockchain* pelo governo do estado de Vermont para autenticar registros oficiais, incluindo documentos judiciais. Este movimento faz parte de um esforço mais amplo para digitalizar e proteger informações oficiais contra alterações não autorizadas²⁵².

A implementação em Vermont incluiu a parceria com empresas de tecnologia para criar um sistema de *blockchain* que possa autenticar documentos judiciais em tempo real. Este sistema permite que qualquer pessoa possa verificar a autenticidade dos documentos utilizando a *blockchain*²⁵³.

²⁵⁰ Digital Dubai. **Dubai Blockchain Strategy**. Disponível em: <https://www.digitaldubai.ae/initiatives/blockchain>. Acesso em: 20 out. 2024.

²⁵¹ Dubai Economy and HSBC Strengthen **UAE KYC Blockchain Platform**. Disponível em: https://ded.ae/News/en/key_news/4772. Acesso em: 20 out. 2024.

²⁵² Vermont General Assembly (2016). **Vermont blockchain enabling act, H.868**. Disponível em: <https://legislature.vermont.gov/bill/status/2016/H.868>. Acesso em: 20 out. 2024.

²⁵³ Vermont General Assembly (2016). **Vermont blockchain enabling act, H.868**. Disponível em: <https://legislature.vermont.gov/bill/status/2016/H.868>. Acesso em: 20 out. 2024.

Entre os desafios, estava a necessidade de assegurar a privacidade dos indivíduos envolvidos nos processos judiciais enquanto se adotava uma tecnologia pública e transparente. A solução adotada envolveu o desenvolvimento de técnicas de criptografia avançadas para proteger informações sensíveis²⁵⁴.

Os benefícios incluem uma maior confiança pública no sistema judicial, aumento na eficiência de administração dos registros judiciais e redução de custos associados à manutenção de arquivos físicos²⁵⁵.

O Arizona seguiu o exemplo, alterando sua Lei de Transações Eletrônicas para incluir assinaturas e registros em *blockchain*, legitimando ainda mais as provas baseadas em *blockchain* nos processos judiciais²⁵⁶.

Compulsando a jurisprudência da corte americana, no caso *United States v. Lizarraga-Tirado*, o Tribunal de Apelações do Nono Circuito abordou a questão da admissibilidade de provas digitais originárias do Google Maps em um processo de imigração²⁵⁷.

A controvérsia central envolvia uma imagem de satélite do Google Earth e um "alfinete" gerado por GPS, que foram apresentados pela promotoria federal para sustentar que o réu, um imigrante sem documentos acusado de entrada ilegal, havia sido capturado em território dos Estados Unidos²⁵⁸.

O réu, por sua vez, alegava ter sido apreendido no lado mexicano da fronteira. Como o ponto principal da defesa era a localização exata da prisão, as

²⁵⁴ Ching, J. (2016). **Is *blockchain* evidence inadmissible hearsay?** Disponível em: <https://www.law.com/sites/almstaff/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/> (Accessed April 19, 2023). Acesso em 20 out. 2024.

²⁵⁵ Buterin, V. (2015). **On public and private *blockchains*.** Disponível em: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> Acesso em 20 out. 2024.

²⁵⁶ Wang X, Wu YC and Ma Z. ***Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes.*** *Front. Blockchain* 7:1306058. doi: 10.3389/fbloc.2024.1306058. 2024.

²⁵⁷ UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (2015). **United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015).** Disponível em: <https://casetext.com/case/united-states-v-lizarraga-tirado>. Acesso em 21 de Out. 2024.

²⁵⁸ UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (2015). **United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015).** Disponível em: <https://casetext.com/case/united-states-v-lizarraga-tirado>. Acesso em 21 de Out. 2024.

provas apresentadas a partir do Google Earth assumiram relevância probatória considerável²⁵⁹.

O juiz Kozinski concluiu que as imagens de satélite, por serem representações factuais, não constituem *hearsay*²⁶⁰, tal como as fotografias. Quanto aos "alfinetes" gerados automaticamente, ele invocou a Regra Federal de Prova 201(b), afirmando que esses marcadores, por serem gerados por software sem intervenção humana, também não poderiam ser considerados *hearsay*. O tribunal, citando precedentes, reforçou que dados gerados por computadores não se enquadram nas regras de *hearsay*²⁶¹.

Quanto ao *blockchain*, que registra eventos com precisão temporal, há semelhança com as imagens do Google Earth. No entanto, a intervenção humana necessária para iniciar transações em *blockchain* introduz uma complexidade adicional, o que pode exigir uma análise distinta em casos futuros de admissibilidade sob as regras de *hearsay*.

Esse precedente reforça a diferença jurídica entre provas testemunhais, sujeitas às normas de *hearsay*, e dados gerados por sistemas computacionais, que são reconhecidos por seu caráter objetivo e pela ausência de influência humana. O conceito de *hearsay* está intrinsecamente vinculado a declarações humanas feitas fora do tribunal, sendo que informações automatizadas por sistemas de computador estão, em regra, isentas dessa classificação²⁶².

²⁵⁹ UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (2015). **United States v. Lizarraga-Tirado**, 789 F.3d 1107 (9th Cir. 2015). Disponível em: <https://casetext.com/case/united-states-v-lizarraga-tirado>. Acesso em 21 de Out. 2024.

²⁶⁰ A norma segundo a qual a testemunha deve depor pelo que sabe per *proprium sensum et non per sensum alterius* impede, em alguns sistemas – como o norte-americano – o depoimento da testemunha indireta, por “ouvir dizer” (*hearsay rule*).

²⁶¹ UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (2015). **United States v. Lizarraga-Tirado**, 789 F.3d 1107 (9th Cir. 2015). Disponível em: <https://casetext.com/case/united-states-v-lizarraga-tirado>. Acesso em 21 de Out. 2024.

²⁶² Knight, E. (2019). **Blockchain jenga: the challenges of blockchain discovery and admissibility under the federal rules**. Hofstra Law Rev. 48 (2), 519–553.

Em termos de legislação, para enfrentar os desafios relacionados à admissibilidade de evidências de *blockchain*, diversos estados dos EUA implementaram mudanças legislativas²⁶³.

Conforme aludido anteriormente, entre fevereiro e março de 2017, o Arizona aprovou uma emenda à Lei de Transações Eletrônicas, que reconhece registros e assinaturas em *blockchain*, garantindo que contratos inteligentes tenham validade legal²⁶⁴.

Delaware, no mesmo período, alterou sua Lei Geral das Corporações, permitindo o uso de redes distribuídas, como *blockchain*, para manter registros empresariais²⁶⁵.

Illinois, com a Lei de Tecnologia *Blockchain*, sancionou o uso da tecnologia em transações e permitiu que os registros gerados por *blockchain* sejam admissíveis como evidência judicial²⁶⁶.

Vermont, em 2016, introduziu o Ato de Facilitação do *Blockchain*, tornando admissíveis no tribunal registros em *blockchain* sem validação externa, desde que respaldados por declaração juramentada²⁶⁷. Embora inovador, esse projeto de lei apresenta desafios, como transferir o ônus de provar a confiabilidade das provas de *blockchain* para a parte contrária e não distinguir entre *blockchains* públicos e privados, o que pode comprometer a qualidade da evidência aceita²⁶⁸.

²⁶³ Fenwick, J., and Vermeulen, K. (2019). **A primer on *blockchain*, smart contracts & crypto-assets from a legal perspective**. SSRN Electron. J., doi:10.2139/ssrn.3488542.

²⁶⁴ Arizona (2017). **Arizona house bill 2417**. Disponível em: <https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf>. Acesso em 21 de Out. 2024.

²⁶⁵ Delaware (2017). **Delaware general corporation law, section 224**. Disponível em: <https://delcode.delaware.gov/title8/c001/sc07/index.html>. Acesso em 21 de Out. 2024.

²⁶⁶ Illinois General Assembly (2020). **Illinois *blockchain* technology act**. Disponível em: <https://www.ilga.gov/legislation/ilcs/>. Acesso em 21 de Out. 2024.

²⁶⁷ Vermont General Assembly (2016). **Vermont *blockchain* enabling act, H.868**. Available at: <https://legislature.vermont.gov/bill/status/2016/H.868>.

²⁶⁸ Wong, M. C. (2021). “***Blockchain* and alternative dispute resolution: opportunities and challenges**,” in **Handbook of *blockchain* law: a guide to understanding and resolving the legal challenges of *blockchain* technology**. Editors P. Hacker, I. Lianos, G. Dimitropoulos, and S. Eich (Cham: Springer International Publishing), 333–345.

3.2.6 Rússia

Não diferindo dos demais Estados, a Federação Russa demonstra ativa participação em meio ao desenvolvimento das tecnologias da informação, a exemplo da publicação do Decreto do Presidente da Federação Russa, de 09.05.2017, nº 203²⁶⁹, "Sobre a Estratégia para o Desenvolvimento da Sociedade da Informação na Federação Russa para 2017-2030", e a Ordem do Governo da Federação Russa, de 28.07.2017, nº 1632-r²⁷⁰, que aprovou o programa "Economia Digital da Federação Russa".

A cidade de Moscou, por meio de um programa existente denominado *Active Citizen*, tem possibilitado que seus residentes votem em diversos assuntos relacionados à administração local²⁷¹.

A tecnologia fora lançada pelo gabinete do prefeito em 2014 e integra a infraestrutura digital da cidade, destacando-se por sua grande visibilidade, sendo frequentemente mencionado na mídia, tanto por receber elogios quanto por gerar controvérsias²⁷².

Segundo o site oficial da plataforma, sua missão é "coletar opiniões" dos cidadãos e "engajá-los" na "vida urbana e no processo de tomada de decisões conduzido pelo governo municipal"²⁷³.

As consultas realizadas na plataforma concentram-se principalmente em eventos da cidade, no desenvolvimento, aperfeiçoamento e embelezamento de espaços públicos, além de recolher feedback sobre propostas políticas e estratégicas

²⁶⁹ Decree of the President of the Russian Federation dated 09.05.2017 No. 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030". Disponível em: <http://www.kremlin.ru/acts/bank/41919>. Acesso em 21 de Out. 2024.

²⁷⁰ Decree of the Government of the Russian Federation dated December 27, 2012 No. 1406 "On the federal target program Development of the Russian judicial system for 2013-2020". Disponível em: <http://consultant.ru>. Acesso em 21 de Out. 2024.

²⁷¹ Zions, J. (2018) "Blockchain Democracy" and the Misleading Promise of Moscow's Active Citizen Program', Disponível em: <https://media.consensys.net/blockchaindemocracy-and-the-misleading-promise-of-moscows-active-citizen-program-2eda7141c5b9>, acesso em 20 Ago. 2024.

²⁷² Zions, J. (2018) "Blockchain Democracy" and the Misleading Promise of Moscow's Active Citizen Program', Disponível em: <https://media.consensys.net/blockchaindemocracy-and-the-misleading-promise-of-moscows-active-citizen-program-2eda7141c5b9>, acesso em 20 Ago. 2024.

²⁷³ Horgan, D. & Dimitrijević, B. (2019) 'Frameworks for Citizens Participation in Planning: From Conversational to Smart Tools', Sustainable Cities and Society, 48.

do governo de Moscou. Com mais de dois milhões de usuários ativos, a plataforma é amplamente promovida como uma ferramenta moderna e eficiente para envolver os cidadãos na gestão urbana, utilizando tecnologia avançada—especialmente o *blockchain*—para assegurar transparência e legitimidade em seus processos. O uso do *blockchain* foi destacado como um avanço significativo na promoção da chamada "democracia em *blockchain*", embora tenha sido alvo de críticas por parte de alguns especialistas²⁷⁴.

O Active Citizen é a plataforma de tecnologia cívica mais utilizada entre as iniciativas patrocinadas pelo Estado em Moscou. Em comparação, em 2019, a plataforma Crowdsourcing contava com 175 mil usuários registrados, Nash Gorod com 1,4 milhão, enquanto o Active Citizen superava 2,5 milhões de usuários, consolidando-se como a mais popular das três. Além disso, a plataforma foi vista como um sucesso em termos burocráticos e está prevista para ser implementada em outras regiões da Rússia²⁷⁵.

Embora o Active Citizen seja apresentado como um instrumento para aprimorar a governança urbana por meio da participação cidadã e promover o empoderamento dos cidadãos no processo decisório, os impactos dessa plataforma devem ser analisados no contexto mais amplo da governança e política de Moscou.

3.3 PERSPECTIVAS PARA A GOVERNANÇA DIGITAL NO PJSC: AVANÇOS, DESAFIOS E A INTEGRAÇÃO DO *BLOCKCHAIN*

A partir da coleta de dados disponíveis pelo Conselho Nacional de Justiça, primariamente, é possível destacar o marco instituído pela Estratégia

²⁷⁴ Holder, S. (2017) 'Can the *Blockchain* Tame Moscow's Wild Politics?', CityLab, 22 December, Disponível em: <https://www.citylab.com/life/2017/12/can-the-blockchain-tame-moscows-wild-politics/547973/>. Acesso em 21 de Ago. 2024.

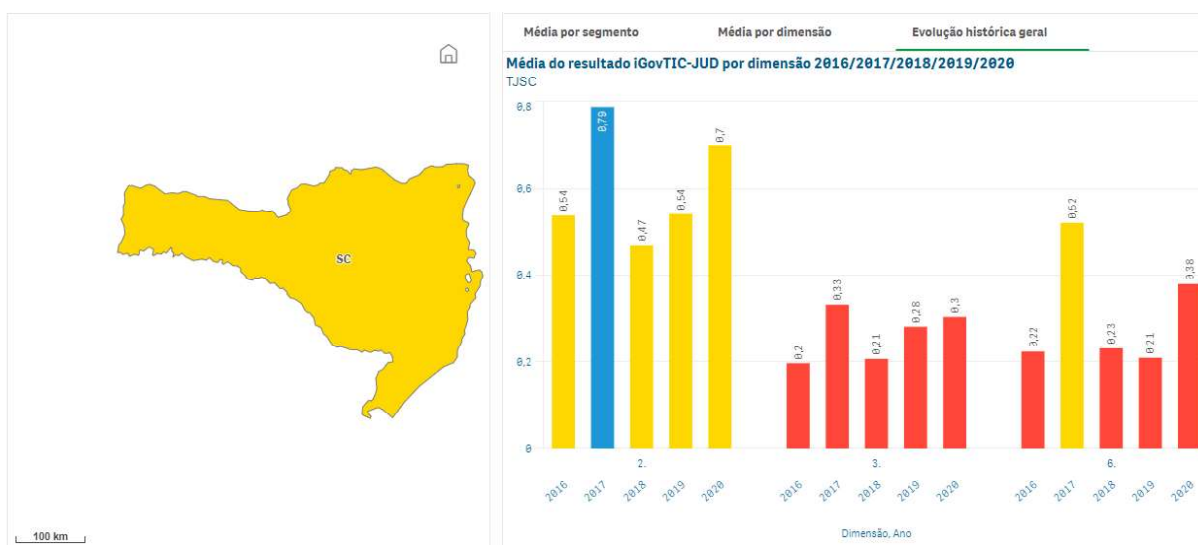
²⁷⁵ Golunov, I. (2018) 'Moskovskii servis "Aktivnyi grazhdanin" zapuskayut na vsyu Rossiyu. Na nem zarabatyvayut chinovniki Rassledovanie Ivana Golunova', Meduza, 25 June, Disponível em: <https://meduza.io/feature/2018/06/25/moskovskiy-servis-aktivnyy-grazhdanin-zapuskayut-na-vsyu-rossiyu-na-nem-zarabatyvayutchinovniki>. Acesso em 21 de Ago. 2024.

Nacional de Tecnologia da Informação e Comunicação (ENTIC-JUD), advinda por meio da Resolução nº 211/2015²⁷⁶.

Junto à implementação da Resolução em 2016, o CNJ deu início ao essencial trabalho de avaliar e cobrar continuamente a evolução do nível de maturidade do programa de governança do Tribunal de Justiça de Santa Catarina, atividade que oportuniza o acompanhamento e consolidação de todas as medidas tomadas desde a época.

Ainda que o diagnóstico operado por meio da aplicação do Índice de Governança, Gestão e Infraestrutura de Tecnologia da Informação e Comunicação do Poder Judiciário (iGovTIC-JUD) sofra contínuas atualizações, ainda assim, é possível compreender uma contínua crescente desde os resultados colhidos a partir de 2016:

Gráfico 9 – Índice de pontuação IGOVTICJUD 2016-2020

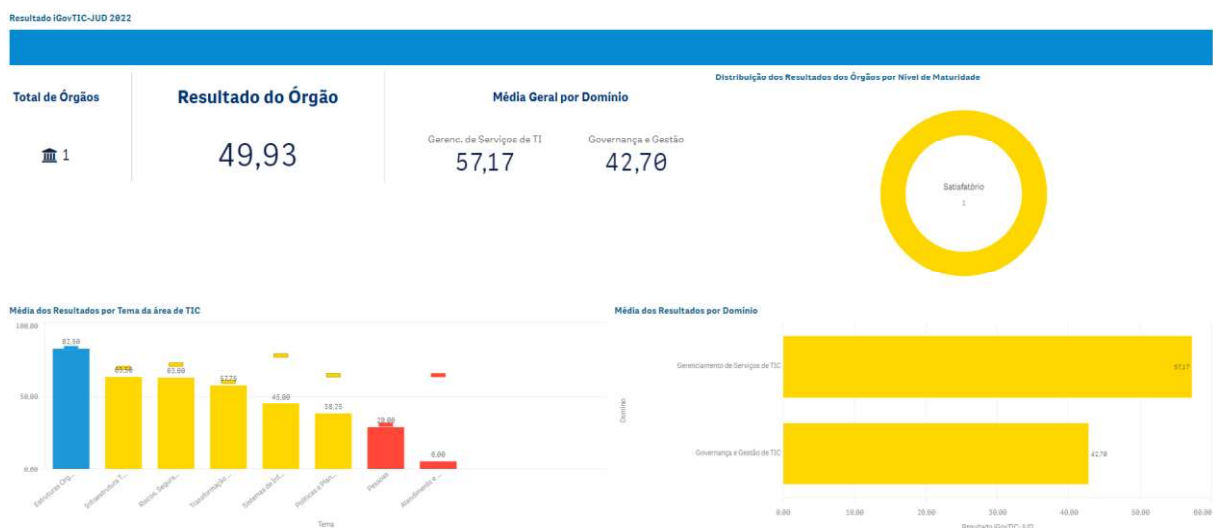


Fonte: Conselho Nacional de Justiça²⁷⁷

²⁷⁶ CONSELHO NACIONAL DE JUSTIÇA. Resolução 211/2015. **Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

²⁷⁷ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2016-2020**. Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=cb200259-f219-48a2-974d-732bc5fe6224&sheet=05258dae-fae2-4ea4-b9ef-1cc55ec52922&theme=Mix_Theme&lang=pt-BR&opt=ctxmenu,currsel. Acesso em: 18 out. 2024.

Gráfico 10 – Índice de pontuação IGOVTICJUD 2021-2024



Resultado iGovTIC-JUD 2024



Fonte: Conselho Nacional de Justiça²⁷⁸

Compulsando os dados expostos acima, verifica-se um contínuo desenvolvimento e aprimoramento do programa de governança digital do PJSC, tanto é verdade que em 2023 obteve a classificação “aprimorado” pela primeira vez desde o início da coleta de dados.

Ao contemplar os pontos identificados ao longo desta pesquisa, desde a fase de elaboração e implementação até o monitoramento e avaliação, evidencia-se a manutenção de um programa periódico de governança digital, com vistas a agregar valor à organização pública, flexível às mudanças inerentes ao processo da transformação digital com constantes e novas tecnologias habilitadoras²⁷⁹.

Sob a ótica da implementação da tecnologia de *blockchain*, nota-se que esta deve ser integrada enquanto uma parceira estratégica para a transformação da organização, de acordo com os seus objetivos.

²⁷⁸ CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2021-2024**. Disponível em: https://paineisanalytics.cnj.jus.br/single/?appid=36047c1e-acf8-4030-8474-78a20bae7c96&sheet=31049d4e-a530-4902-b1ed-6cb77477d5fa&theme=cnj_theme&select=Ano,2024. Acesso em: 18 out. 2024.

²⁷⁹ COELHO, Claudio Carneiro B. P. **Análise da Efetividade dos Programas de Compliance**. In: GRC Governança, risco e compliance: temas contemporâneos: aspectos teóricos e práticos. Rio de Janeiro: Lumen Juris, 2022.

A temática recebe relevância, uma vez que, foi possível perceber, de maneira geral, as principais necessidades do programa de governança digital do PJSC, sendo os pontos de destaque:

- Minimizar os riscos de continuidade do negócio por meio da implantação da governança e gestão da Segurança da Informação institucional, além da capacitação e conscientização contínua de magistrados e servidores;

- Aperfeiçoar e normatizar atividades para aumentar padronização, segurança e produtividade.

- Fortalecer a Segurança da Informação com ações que mitiguem vulnerabilidades nos serviços de TIC.

- Promover capacitação contínua das equipes de TI em Segurança da Informação.

- Priorizar ações para aumentar a capacidade produtiva da DTI na evolução do eproc.

- Promover a renovação dos equipamentos de informática.

- Centralizar serviços selecionados em um único aplicativo para dispositivos móveis.

- Racionalizar a força de trabalho através de atividades remotas e otimização de funções subaproveitadas.

- Manter o site institucional atualizado, ampliando finalidades e melhorando a funcionalidade.

- Realizar Auditoria Interna, no mínimo, anualmente quanto a eficácia dos controles da Governança e da Gestão de TIC, inclusive nos aspectos relativos aos riscos afetos à segurança da informação, aos serviços judiciais e aos demais ativos de TIC críticos do órgão.

Nota-se que, com a implementação da tecnologia *blockchain* no programa de governança digital do Poder Judiciário de Santa Catarina (PJSC), haveria ganhos notórios de segurança, transparência, integridade de dados e eficiência operacional.

A estrutura descentralizada e resistente a alterações de registros imutáveis e auditáveis garante a proteção dos dados sensíveis dos cidadãos, de forma que promoveria a confiança pública nos processos judiciais e cumpriria com a própria missão institucional do órgão.

Noutro norte, o *blockchain* igualmente eleva o padrão de proteção contra ataques cibernéticos, um benefício crucial, considerando a crescente ameaça de incidentes de segurança digital que o Judiciário brasileiro enfrenta.

Em nível nacional, exemplos como o Tribunal de Justiça do Maranhão (TJMA) demonstram que o uso de *blockchain* pode assegurar a autenticidade e a integridade dos registros processuais, criando um sistema confiável para autenticação e armazenamento de documentos judiciais. Essa prática já resultou em melhorias operacionais ao reduzir o tempo e o custo com a validação de informações, além de contribuir para uma maior segurança dos dados.

No cenário internacional, vários países apresentam casos de sucesso que servem de inspiração para o PJSC, a exemplo do sistema de governança digital estoniano que utiliza *blockchain* para registros de saúde, identidade e registros judiciais, promovendo um ambiente em que os cidadãos podem acessar de forma transparente as informações que lhes dizem respeito. A integração com contratos inteligentes possibilita automatizar certos processos judiciais, agilizando a tramitação de casos e reduzindo a carga burocrática.

Dubai, por sua vez, estabeleceu a meta de implementar a *blockchain* na administração pública, abrangendo transações e registros judiciais, proporcionando um sistema acessível e transparente para os cidadãos e garantindo a inviolabilidade dos registros digitais. Esse exemplo pode orientar o PJSC na criação de um ambiente digital em que contratos e registros judiciais sejam automatizados e acessíveis, resultando em mais transparência e acessibilidade para os cidadãos.

Tratando-se dos princípios de acesso à justiça e celeridade processual, em cidades como Hangzhou na china, a qual utilizou da *blockchain* em tribunais de Internet para a resolução de disputas digitais e autenticação de evidências online. Esse uso inovador permite que evidências digitais, como contratos eletrônicos e informações transacionais, sejam autenticadas de maneira segura e rápida, utilizando a *blockchain* para verificar a procedência e a integridade dos dados. Esse modelo pode inspirar o PJSC a adotar a *blockchain* para autenticação de provas digitais, aumentando a credibilidade dos registros e o tempo de resposta em litígios.

A exemplo da África do Sul que empregou *blockchain* em diversos serviços públicos, incluindo o sistema judicial, com foco na segurança dos registros e na verificação de identidades, o PJSC poderia explorar o caso ao implementar a *blockchain* para registro seguro de dados de usuários e partes envolvidas, garantindo privacidade e segurança.

Nesse sentido, verifica-se que o estabelecimento de um programa de governança digital alinhado estrategicamente às novas tecnologias de segurança da informação, tal como o caso da *blockchain* debatido na presente dissertação, resulta diretamente no auxílio do cumprimento das atividades e metas do órgão, apresentando benefícios como o apoio à tomada de decisão para o gestor, maior eficiência na prestação de serviços à sociedade pelo meio digital, aumento da eficiência no desenvolvimento e desempenho das atividades internas, maior agilidade e celeridade da Administração Pública, maior engajamento e incentivo à inovação entre os servidores e sociedade e, sobretudo, da garantia da segurança da informação.

Em outros termos, a *blockchain* e as tecnologias da informação em geral, assim como o programa de governança, devem ser visualizados enquanto um investimento e como ferramentas aptas para gerar soluções adequadas à realidade e aos problemas enfrentados tanto pelo PJSC quanto pela sociedade.

CONSIDERAÇÕES FINAIS

A presente pesquisa buscou analisar a ascensão de direitos fundamentais frente a evolução de novas tecnologias, assim como da maturidade do atual programa de governança digital do Poder Judiciário de Santa Catarina, tendo em vista as fragilidades experimentadas pelos sistemas utilizados no Poder Judiciário como um todo.

Por fim, objetivou-se situar a operacionalização da *blockchain* e a atual exploração da mesma frente aos tribunais nacionais e governos internacionais, assim como fora proposta uma análise crítica sobre a maturidade do programa de governança digital do Poder Judiciário de Santa Catarina (PJSC) e a viabilidade da aplicação da tecnologia *blockchain* para mitigar riscos cibernéticos, proteger dados pessoais e garantir uma maior transparência e eficiência no tratamento jurisdicional.

Ao estudar o contexto histórico e legislativo da governança digital, aliado à ascensão de tecnologias disruptivas como a *blockchain*, o trabalho buscou expor como essas inovações tecnológicas podem ser aplicadas para assegurar direitos fundamentais em um ambiente jurídico cada vez mais digital e globalizado.

No Capítulo 1, trata-se da contextualização histórica e jurídica que envolve o desenvolvimento da governança digital, com foco no Poder Judiciário de Santa Catarina (PJSC). Parte-se de uma análise das revoluções industriais e como cada uma dessas fases representou não apenas uma transformação econômica e

tecnológica, mas também uma mudança estrutural na organização da sociedade, que por sua vez influenciou diretamente as normativas jurídicas.

Ao traçar esse paralelo histórico, o capítulo destaca como o progresso tecnológico, especialmente nas últimas décadas, trouxe novas demandas e desafios para a proteção de direitos fundamentais, como a privacidade e a segurança dos dados.

É cediço que as inovações tecnológicas abarcadas na gestão das organizações são inseparáveis de seu cotidiano, caso em que não se diferencia da utilização de *softwares* destinados à gestão do judiciário.

Apesar dos diversos avanços e automatizações trazidos por meio da inserção de tecnologias, todo o globo vem sendo frequentemente afetado por ataques cibernéticos, tema que toma grande relevância nas discussões sobre os riscos atrelados ao desenvolvimento de *softwares* e tecnologias em geral, bem como da necessidade de implementar robustas medidas técnicas e prover a manutenção de um rígido programa de Compliance Digital, a fim de mitigar os mencionados riscos²⁸⁰.

Conforme destacado, a temática recebe relevância a partir do ataque cibernético sofrido pelo Superior Tribunal de Justiça²⁸¹ em 03/11/2020, o qual foi considerado o maior incidente em face de instituição judiciária brasileira até então, de forma que toda a operacionalização das demandas judiciais foi suspensa e o restabelecimento da distribuição de processos ocorreu apenas 168 horas após o ocorrido, levando-se em conta uma extensa força tarefa montada para responder o incidente.

²⁸⁰ CATELLI, Maria Augusta Peres; IDIE; Renata Yumi. Prevenir para Mitigar: a importância do desenvolvimento de cultura de segurança cibernética nas organizações. In: BLUM, Renato Opice; WAJSBROT, Shirly (org.). Cyber Risk Estratégias: **estratégias nacionais e corporativas sobre riscos e segurança cibernética**. São Paulo: Thompson Reuters Brasil, 2020. Cap. 1.

²⁸¹ SUPERIOR TRIBUNAL DE JUSTIÇA. **Comunicado da Presidência do STJ**. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em 10 de mai. 2022.

Os incidentes não findaram com o episódio narrado acima, os órgãos do judiciário têm se mostrado alvos de ataques hackers, dentre eles destacam-se eventos ocorridos nos sistemas do TJRS²⁸², TSE²⁸³ e TRF1²⁸⁴.

Ademais, não bastasse isso, segundo a consultoria alemã Roland Berger, o Brasil foi o 5º país que mais sofreu ataques cibernéticos em 2021²⁸⁵.

Neste sentido, cabe expor o recente relatório produzido pela IBM²⁸⁶, o qual apontou que o custo médio causado por uma violação de dados no Brasil foi de U\$1,08 milhões no ano de 2021, considerando gastos destinados aos fatores de detecção e escalabilidade (investigação forense, auditoria, gerenciamento de crise), notificação (e-mails, chamadas, avisos para os titulares, órgãos reguladores e especialistas externos), resposta pós-violação (equipe de atendimento, serviços de monitoramento, emissão de novas contas, despesas legais, multas de autoridades públicas) e negócio perdido interrupção dos negócios e perda por tempo de inatividade do sistema, custo de clientes perdidos e perda de reputação.

A governança digital emerge nesse contexto como uma necessidade, não apenas para o setor privado, mas principalmente para instituições públicas como o Judiciário, que lida diariamente com grandes volumes de informações sensíveis.

Nesse sentido, o capítulo examina como as transformações tecnológicas, principalmente no Brasil, conduziram à criação de marcos regulatórios específicos, como a Lei Geral de Proteção de Dados (LGPD), e como esses diplomas

²⁸² TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. **Nota de esclarecimento**. Disponível em: <https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/>. Acesso em: 05 de mai. 2022.

²⁸³ TRIBUNAL SUPERIOR ELEITORAL. **TSE institui comissão presidida por Alexandre e Moraes para acompanhar investigações sobre ação de hackers contra o processo eleitoral**. Disponível em: <https://www.tse.jus.br/imprensa/noticias-tse/2020/Novembro/tse-institui-comissao-presidida-por-alexandre-de-moraes-para-acompanhar-investigacoes-sobre-acao-de-hackers-contra-o-processo-eleitoral?SearchableText=HACKER>. Acesso em: 05 de mai. 2022.

²⁸⁴ CNN. **Sob suspeita de ataque hacker, TRF-1 blinda sistema eletrônico**. Disponível em: <https://www.cnnbrasil.com.br/nacional/sob-suspeita-de-ataque-hacker-trf-1-blinda-sistemaeletronico/>. Acesso em: 05 de mai. 2022.

²⁸⁵ ISTOÉ DINHEIRO. **Brasil foi 5º país com mais ataques cibernéticos no ano: lembre os principais**. Disponível em: <https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/>. Acesso em: 10 de mai. 2022.

²⁸⁶ IBM. **Quanto custa uma violação de dados**. Disponível em: <https://www.ibm.com/br-pt/security/data-breach>. Acesso em: 05 de mai. 2022.

legais moldam a forma de atuação dos órgãos públicos em sua relação com a sociedade digital.

O capítulo explora também os primeiros passos do PJSC na adoção de soluções digitais, destacando os esforços para modernizar sua estrutura e melhorar a eficiência de seus serviços por meio da digitalização de processos. No entanto, são identificados desafios importantes, como a adequação à governança digital e a necessidade de um alinhamento mais claro com as diretrizes estabelecidas pelo Conselho Nacional de Justiça (CNJ).

Esse contexto inicial serve de base para a análise dos capítulos seguintes, que discutirão a tecnologia *blockchain* como uma ferramenta estratégica para enfrentar esses desafios.

O Capítulo 2 aprofunda-se na tecnologia *blockchain*, uma das principais inovações disruptivas da era digital. A *blockchain*, que teve sua origem no setor financeiro com a criação do Bitcoin, evoluiu para muito além das criptomoedas, ganhando relevância como uma solução para questões de segurança, transparência e imutabilidade em diferentes áreas, incluindo o setor público.

A *blockchain* é apresentada em sua essência técnica, com explicações detalhadas sobre sua estrutura descentralizada e a forma como ela assegura a integridade dos dados por meio de um sistema de registros distribuídos.

Após essa introdução técnica, o capítulo explora os possíveis benefícios de se aplicar a *blockchain* no contexto do PJSC. O principal argumento reside na capacidade da *blockchain* de aumentar a transparência e a auditabilidade dos processos, mitigando riscos cibernéticos e garantindo a proteção de dados pessoais.

A tecnologia possibilita a criação de registros imutáveis, ou seja, qualquer dado inserido em uma *blockchain* não pode ser alterado, o que garante a confiança nos sistemas judiciais e evita fraudes. Além disso, a *blockchain* permite a automação de processos por meio dos contratos inteligentes (smart contracts), que podem ser utilizados para otimizar procedimentos judiciais, reduzindo burocracias e aumentando a eficiência.

Outro ponto central abordado no capítulo abarca a segurança cibernética frente às crescentes ameaças digitais, sendo que a *blockchain* surge como uma ferramenta capaz de proporcionar uma camada adicional de proteção, especialmente no que tange à prevenção de vazamentos de dados.

No entanto, faz-se igualmente um levantamento dos desafios relacionados à implementação dessa tecnologia no Judiciário, tal como a necessidade de investimentos em infraestrutura tecnológica, a capacitação dos servidores e a superação de barreiras culturais e legislativas.

Por fim, o Capítulo 3 buscou expandir os horizontes da investigação ao estudar casos concretos de aplicação da *blockchain* em tribunais e governos, tanto no Brasil quanto em outros países.

A metodologia adotada envolve uma análise comparativa entre tribunais brasileiros que iniciaram a implementação da *blockchain* em suas atividades administrativas e judiciais e experiências internacionais em nações que estão na vanguarda da utilização dessa tecnologia no setor público.

No cenário nacional, são destacados tribunais como o Tribunal de Justiça de São Paulo (TJSP), o Tribunal de Contas da União (TCU) e o Tribunal de Justiça do Estado de Goiás, que começaram a experimentar a *blockchain* em processos administrativos e judiciais. Essas iniciativas são descritas como exemplos pioneiros de como a *blockchain* pode ser aplicada no Brasil para aprimorar a segurança e a eficiência do Judiciário. Cada tribunal enfrentou desafios específicos, mas os resultados obtidos até o momento indicam que há um enorme potencial para expandir o uso dessa tecnologia.

Em nível internacional, o terceiro capítulo abarca a análise de países como a Estônia, que se tornou referência global em governança digital, implementando a *blockchain* em praticamente todos os aspectos da administração pública.

Malta, conhecida como "ilha *blockchain*", é outro exemplo de como a tecnologia pode ser utilizada para fomentar um ambiente regulatório amigável à inovação, inclusive no setor judicial.

Por sua vez, o estudo de Dubai e dos Estados Unidos, que também avançaram significativamente na adoção da *blockchain*, reforça a importância da modernização digital no setor público como uma forma de aumentar a transparência e a confiança no governo.

A análise comparativa revela lições importantes para o PJSC, um dos pontos destacados é que a aplicação da *blockchain* depende não apenas da tecnologia em si, mas de um ambiente regulatório e institucional que favoreça a inovação.

Nesse sentido, os resultados obtidos a partir dos estudos de caso constantes no terceiro capítulo sugerem que a experiência destes países pode servir de modelo para a implementação da *blockchain* no Judiciário catarinense, desde que haja um planejamento estratégico sólido e uma vontade política para superar os obstáculos iniciais.

Quanto à confirmação ou não das hipóteses inicialmente levantadas, quais sejam: a) Esperava-se a localização de diversas ações de melhoria necessárias ao programa de governança digital do PJSC, melhorias das quais ressoarão em: a) maior aderência ao cumprimento legal e tutela do direito fundamental garantido pela Constituição Federal à massiva quantidade de indivíduos envolvidos nas operações de tratamento de dados do PJSC; b) desenvolvimento e alçada da maturidade do programa de Compliance Digital e; c) a mitigação de ameaças cibernéticas a partir da inibição dos riscos levantados e a consequente proteção do patrimônio do PJSC, tanto no que se refere à reputação do órgão e montante econômico presente no ativo informacional detido pelo mesmo, quanto no amortecimento de gastos decorrentes de incidentes de segurança e vazamentos de dados, os quais se provaram exorbitantes e complexos; e b) Acreditava-se que a aplicação da tecnologia de *blockchain* em inclusão ao pilar de segurança da informação do programa de governança favorece a concretização do ODS16 na promoção de sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionando o acesso à justiça para todos e construindo instituições eficazes, responsáveis e inclusivas em todos os níveis, foram parcialmente confirmadas.

Por um lado, restou evidenciado que a implementação da tecnologia *blockchain* no Judiciário catarinense tem implicações que vão muito além do âmbito tecnológico, envolvendo também transformações sociais e políticas profundas. Do ponto de vista social, o uso da *blockchain* pode trazer uma nova era de transparência e confiança no sistema judiciário. Ao garantir a imutabilidade dos registros processuais, a *blockchain* permite que todas as partes envolvidas em um processo judicial — desde cidadãos até advogados e magistrados — tenham a certeza de que os dados e documentos processuais são invioláveis e estão devidamente protegidos contra fraudes ou manipulações. Isso fortalece a confiança pública no sistema de justiça e pode contribuir para a redução de conflitos e desconfianças na administração de processos.

No campo político, a adoção da *blockchain* alinha-se diretamente com os Objetivos de Desenvolvimento Sustentável (ODS) da ONU, em especial o ODS 16, que busca promover sociedades justas, pacíficas e inclusivas. Ao utilizar a *blockchain*, o Judiciário não apenas fortalece a segurança e a eficiência de seus sistemas, mas também se posiciona como um agente ativo na construção de instituições públicas mais transparentes e confiáveis. Isso pode ter repercussões significativas nas discussões sobre governança digital no Brasil, incentivando outros órgãos públicos a adotarem medidas semelhantes e fomentando um debate mais amplo sobre a necessidade de modernização do Estado para acompanhar as demandas da sociedade digital.

Por fim, no âmbito tecnológico, a *blockchain* representa uma das soluções mais inovadoras e promissoras da atualidade, com um vasto potencial de aplicação no setor público. Sua capacidade de assegurar a integridade dos dados, garantir auditorias seguras e promover a interoperabilidade entre diferentes sistemas administrativos e judiciais pode revolucionar a forma como o Judiciário opera. Além disso, ao promover a transparência e a eficiência, a *blockchain* pode ser um catalisador para a transformação digital de outras áreas do governo, criando um efeito dominó que pode beneficiar todo o setor público brasileiro. A implantação de uma solução tecnológica tão avançada também abre portas para novos investimentos e parcerias público-privadas no desenvolvimento de soluções digitais que beneficiem tanto o governo quanto os cidadãos.

Por outro lado, sob o viés da adoção da tecnologia *Blockchain* no Judiciário de Santa Catarina, apesar de promissora, confronta-se com desafios substanciais que demandam um planejamento estratégico minucioso, investimento em infraestrutura, atualização legislativa, e uma considerável mudança cultural e organizacional, cenário agravado ao analisar os resultados dos testes de maturidade do PJSC, incluindo o mesmo em uma das piores qualificações dentre todos os programas dos demais tribunais brasileiros.

Nesse diapasão, verifica-se que os objetivos específicos da pesquisa foram atingidos, a pesquisa evidenciou que a governança digital do PJSC, embora sólida em muitos aspectos, ainda necessita de aprimoramentos significativos, especialmente no que tange à proteção de dados pessoais e à prevenção de riscos cibernéticos.

A tecnologia *blockchain*, ao ser incorporada nesse cenário, se apresenta como uma solução inovadora e eficiente para superar esses desafios, contribuindo para a melhoria dos processos judiciais e a proteção dos direitos fundamentais.

O impacto positivo de sua implementação pode transcender o Judiciário catarinense, tornando-se um exemplo de sucesso para outras instituições públicas no Brasil e no exterior.

Por fim, destaca-se que a presente pesquisa não teve a intenção de esgotar a temática, porém, contribuir e estimular a elaboração de novos estudos e investigações acerca da contínua missão de melhoria do programa de governança digital do PJSC, especialmente em razão da missão institucional acerca da proteção e privacidade de dados, assim como da promoção de uma sociedade pacífica e inclusiva ao desenvolvimento sustentável, intentando-se proporcionar o acesso à justiça para todos por meio de instituições eficazes.

REFERÊNCIA DAS FONTES CITADAS

AEDTNI – Associação de Empresas de Desenvolvimento Tecnológico Nacional e Inovação. **Brasil está entre os 20 países com melhor oferta de serviços públicos digitais**. Disponível em: <https://pedbrasil.org.br/brasil-esta-entre-os-20-paises-com-melhor-oferta-de-servicos-publicos-digitais/>. Acesso em: 09 nov. 2023.

ALCÂNTARA, L. T. et al. **Uso da tecnologia *Blockchain* como instrumento de governança eletrônica no setor público**. In: II CONGRESSO INTERNACIONAL DE CONTABILIDADE PÚBLICA, Lisboa, 2019. Anais [...]. Lisboa, PT, 2019. Disponível em: https://repositorio.unb.br/bitstream/10482/34651/1/EVENTO_UsoTecnologiaBlockchain.pdf. Acesso em: 7 jun. 2024.

ASHOK, I. (2017). **“Silicon Valley translation firm with Google, Boeing and other clients hit with data leak”**, International Business Times UK, Disponível em: <https://www.ibtimes.co.uk/silicon-valleytranslation-firm-google-boeing-other-clients-hit-data-leak-1602177> Acesso em 20 Mai. 2024.

Ast, F., & Sewrjugin, A. (2015). **The crowdjury, a crowdsourced justice system for the collaboration era**. Crowdjury Org, 1(9), 1689–1699.

BAKSHI, Vikram A.; BRAINE, Lee; CLACK, Christopher Clack. **Smart Contract Templates: Foundations, design landscape and research directions**. Aug. 4, 2016. Disponível em: https://www.researchgate.net/publication/305779577_Smart_Contract_Templates_foundations_design_landscape_and_research_directions_CDClack_VABakshi_and_LBraine_arxiv160800771_2016/link/5924238ea6fdcc4443ff2f6a/download. Acesso em: 19 out. 2024.

BEZERRA, Tiago José de Souza Lima. **A constitucionalização da democracia digital no direito brasileiro: a regulação das políticas e estratégias de governança digital na Administração Pública Federal**. 192 fls. 2020. Dissertação (Mestrado em Direito). Programa de Pós-graduação em Direito da Universidade Federal do Rio Grande do Norte. Natal, 2020, p. 137. Disponível em: <https://repositorio.ufrn.br/handle/123456789/31720>. Acesso em: 06 out. 2024.

BELCHIOR, R., Correia, M., & Vasconcelos, A. (2019). **Justicechain: using *blockchain* to protect justice logs**. Lecture Notes in Computer Science, 11877, 318-325. doi:10.1007/978-3-030-33246-4_21.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. 423 p.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 abr. 2023.

BRASIL. Decreto nº 9.203, de 22 de novembro de 2017. **Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em: 06 out. 2024.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. **Institui a Estratégia Nacional de Segurança Cibernética (ENSC).** Diário Oficial da União, Brasília, 5 fev. 2020.

BRASIL. Decreto nº 10.332, de 28 de abril de 2020. **Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.** Brasília, DF: Presidência da República, 2020. Disponível em: <https://www.in.gov.br/web/dou/-/decreto-n-10.332-de-28-de-abril-de-2020-254430358>. Acesso em: 05 mai. 2022.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.** Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 26 de outubro de 2023.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 05 mai. de 2023.

BRASIL. Tribunal de Contas da União. **Levantamento da tecnologia *blockchain*.** Brasília: TCU, Secretaria da Sessões (Seses), 2020.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília, 5 out. 1988.

BRYNJOLFSSON, Erik; MCAFFE, Andrew. **The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.** W Norton & Company, 2014.

BUZ, Marcelo. **A importância da identificação digital segura: confiança.** In: BLUM, Renato Opice; WAJSBROT, Shirley (org.). *Cyber Risk Estratégias: estratégias nacionais e corporativas sobre riscos e segurança cibernética.* São Paulo: Thompson Reuters Brasil, 2020. Cap. 3. p. 61-85.

CÂMARA DE MALTA. ***Blockchain, The New Regulatory Framework.*** Disponível em: <https://www.maltachamber.org.mt/en/blockchain-the-new-regulatory-framework>

CAHF. 2020. **Exploring Technology in Residential Property Markets.** Centre for Affordable Housing Finance Africa.

CATHOLICA UNIVERSITY OF MINAS GERAIS. EDGE, Charles; O'DONNELL, Daniel. **Introduction to cryptography.** In: LOPES, Marcus Vinícius Pimenta. *A participação ativa do acusado na persecução que utiliza a busca e a apreensão de*

elementos de provas digitais. Tese de Doutorado. 218 f. Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023. p. 73

CATELLI, Maria Augusta Peres; IDIE; Renata Yumi. **Prevenir para Mitigar: a importância do desenvolvimento de cultura de segurança cibernética nas organizações**. In: BLUM, Renato Opice; WAJSBROT, Shirley (org.). *Cyber Risk Estratégias: estratégias nacionais e corporativas sobre riscos e segurança cibernética*. São Paulo: Thompson Reuters Brasil, 2020. Cap. 1.

CHANG, Anne; ALMEIDA, Cynthia Barbosa de. **Blockchain e proteção de dados**. In: PALHARES, Felipe. *Temas atuais de Proteção de Dados*. São Paulo: Thompson Reuters Brasil, 2020. Cap. 3.

CHING, J. (2016). **Is blockchain evidence inadmissible hearsay?** Disponível em: <https://www.law.com/sites/almstaff/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/>. Acesso em: 19 mai. 2024.

CINNHE, J. **Sob suspeita de ataque hacker, TRF-1 blinda sistema eletrônico**. Disponível em: <https://www.cnnbrasil.com.br/nacional/sob-suspeita-de-ataque-hacker-trf-1-blinda-sistema-eletronico/>. Acesso em: 05 de mai. 2022.

CLUBDA, Daniela Emiliano de. **Planejando a Transformação Digital 4.0**. In: FERNANDES, Aguinaldo Aragon; DINIZ, Jose Luis; ABREU, Vladimir Ferraz de. (Coords.). *Governança Digital 4.0*. Rio de Janeiro: Brasport, pp. 206-220, 2019.

COELHO, Claudio Carneiro B. P. **Análise da Efetividade dos Programas de Compliance**. In: *GRC Governança, risco e compliance: temas contemporâneos: aspectos teóricos e práticos*. Rio de Janeiro: Lumen Juris, 2022.

COINDESK. **Malta Passes Three Bills on Blockchain and Crypto Assets**. Disponível em: <https://www.coindesk.com/malta-passes-three-bills-on-blockchain-and-crypto-assets>.

CONSELHO DA EUROPA. **Manual da Legislação Europeia de Proteção de Dados**. 2014, ISBN 978-92-871-9939-3. Disponível em: http://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf. Acesso em: 09 de mai. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Acordo de Cooperação Técnica n.º 133/2024, celebrado entre o Conselho Nacional de Justiça e a Associação Brasileira de Criptoconomia**. Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_org_ao_acesso_externo=0. Acesso em: 20 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Resolução 211/2015. Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Diário de Justiça [da] União: CNJ, Brasília, DF, 16 dez. 2015. Disponível em: <https://www.cnj.jus.br>. Acesso em: 15 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 370, de 28 de janeiro de 2021. **Estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3706>. Acesso em: 15 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2018**. Disponível em: <https://www.tjsc.jus.br/documents/840056/4196365/Levantamento+iGovTIC-Jud+2018+-+Resultado+CNJ/1109afbd-1624-6eab-1c1e-1cf0bf24a2c6>. Acesso em: 18 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário iGovTIC-JUD2023**. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2023/10/relatorio-geral-do-igovtic-jud-2023-2023-09-27-v2.pdf>. Acesso em: 18 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **MA: Centro de Inteligência do Judiciário discute projetos de tecnologia e inovação**. CNJ, 30 dez. 2021. Disponível em: <https://www.cnj.jus.br/ma-centro-de-inteligencia-do-judiciario-discute-projetos-de-tecnologia-e-inovacao/>. Acesso em: 14 out. 2024.

COLLINGRIDGE, D. (1980). **The social control of technology**. New York: St. Martin's Press.

COUTO, Militello Gabriel. **Educação e pensamento computacional: Estudo de caso sobre E- Estônia**. Relatório final de pesquisa. PUCSP, São Paulo. 2016.

CRISTÓVAM, José Sérgio da Silva; SAIKALI, Lucas Bossoni; SOUSA, Thanderson Pereira de. **Governo Digital na implementação de serviços públicos para a concretização de direitos sociais no Brasil**. Sequência. Florianópolis, n. 84, pp. 209-242, abr. 2020, p. 212. Disponível em: <https://www.scielo.br/j/seq/a/f9mk84ktBCQJFzc87BnYgZv/?format=pdf&lang=pt>. Acesso em: 20 out. 2024.

DAL RI, Luciene. **O COSTUME CONSTITUCIONAL NO BRASIL IMPÉRIO PARA A CONSTRUÇÃO DO ESTADO DE DIREITO?**. HISTORIA CONSTITUCIONAL (OVIEDO), v. 1, p. 1257-1275, 2024.

DO4AFRICA. **Project Description**. Disponível em: <https://www.do4africa.org/en/projets/bitland-2/>

EDGE, Charles; O'DONNELL, Daniel. **Introduction to cryptography**. In: LOPES, Marcus Vinícius Pimenta. A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de provas digitais. Tese de Doutorado. 218 f. Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023. p. 73

ENCCLA – ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E À LAVAGEM DE DINHEIRO. **Blockchain no setor público: guia de conceitos e usos potenciais**. [Brasília, DF], 2020. Disponível em:

<http://enccla.camara.leg.br/acoes/arquivos/resultados-enccla-2020/blockchainno-setor-publico-guia-de-conceitos-e-usos-potenciais/view>. Acesso em: 22 maio 2024.

FERREIRA, J. E.; PINTO, F. G. C.; DOS SANTOS, S. C. **Estudo de mapeamento sistemático sobre as tendências e desafios do Blockchain**. Gestão. Org., [s.l.], v. 15, n. 6, p. 108-117, 2017. Disponível em: <https://periodicos.ufpe.br/revistas/gestaoorg/article/view/231244>. Acesso em: 19 mai. 2024.

FERNANDA, Aguinaldo Aragon. **A Governança Digital 4.0**. In: FERNANDES, Aguinaldo Aragon; DINIZ, José Luís; ABREU, Vladimir Ferraz de. (Coords.). Governança Digital 4.0. Rio de Janeiro: Brasport, pp. 160-205, 2019, p. 202.

FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços**. 2. ed. Rio de Janeiro: Brasport, 2008.

FERNANDES, Aguinaldo Aragon; BRITO, Ronaldo; SOUZA, Daniela Emiliano de. **Planejando a Transformação Digital 4.0**. In: FERNANDES, Aguinaldo Aragon; DINIZ, Jose Luis; ABREU, Vladimir Ferraz de. (Coords.). Governança Digital 4.0. Rio de Janeiro: Brasport, pp. 206-220, 2019.

FERNEDA, Ariê Scherreier. **Governança e transformação digital nas capitais dos estados brasileiros: as Tecnologias da Informação e Comunicação como aliadas estratégicas da Administração Pública Municipal**. 225 fls. 2023. Dissertação (Mestrado em Direito). Universidade Federal de Santa Catarina. Florianópolis, 2023.

FERNEDA, Ariê Scherreier; CRISTÓVAM, José Sérgio da Silva. **Metodologias ágeis para a transformação digital no Brasil: uma análise do Scrum aplicado ao Setor Público**. Direitos Democráticos & Estado Moderno – Revista da Faculdade de Direito da PUC-SP. São Paulo, v. 3, n. 6, pp. 84-101, set./dez. 2022. Disponível em: <https://revistas.pucsp.br/DDEM/article/view/58498>. Acesso em: 19 out. 2024.

FREITAS, Juarez; TEIXEIRA, Anderson Vichinkeski. **Democracia digital e avaliação continuada de políticas públicas**. Revista Brasileira de Estudos Políticos. Belo Horizonte, n. 119, pp. 227-252, jul./dez. 2019. Disponível em: <https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/715>. Acesso em: 22 jun. 2024.

GALERY, Augusto Dutra; ALBERTIN, Alberto Luiz. Inclusão Digital. In: ALBERTIN, Alberto Luiz; MOURA, Rosa Maria (Org.). **Tecnologia da Informação**. 1. ed. 2. reimp. São Paulo: Atlas, 2007, pp. 242-254.

GARTNER. **Key Issues For Business Process Management**. 2008. Disponível em: <https://www.gartner.com/en/documents/620810>. Acesso em: 15 out. 2024.

GODEY, Maria. **Blockchain aplicada aos contratos inteligentes: perspectivas empresariais e natureza jurídica**. In: LIMA, Ana Paula M. Direito digital: Debates contemporâneos. São Paulo: Thompson Reuters Brasil, 2019.

GOMES, Danusa Fernandes Rufino. **Governança Digital: desenvolvimento de um índice para autarquias públicas federais vinculadas ao Ministério da Educação**. 162 fls. 2018. Dissertação (Mestrado em Administração Pública). Programa de Pós-graduação em Administração Pública da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da Universidade de Brasília. Brasília, 2018, p. 56. Disponível em: <https://repositorio.unb.br/handle/10482/32724>. Acesso em: 06 out. 2024.

GOMES, V. J. F.; UCHOA, S. B. B.; SANTOS, T. F. S. **Mapeamento tecnológico das patentes desenvolvidas a partir da tecnologia *Blockchain*: um cenário global**. Cadernos de Prospecção, Salvador, v. 11, n. 4, p. 1.166-1.181, dezembro, 2018. Disponível em: <https://periodicos.ufba.br/index.php/nit/article/view/27193>. Acesso em: 24 mai. 2024.

GOVERNANÇA DIGITAL NAS CAPITALS. **Desenvolvimento de um índice para autarquias públicas federais vinculadas ao Ministério da Educação**. Disponível em: [URL não fornecida].

GOVERNO DA ESTÔNIA. (2018). **E-ESTONIA**. Disponível em: <https://e-estonia.com/>.

GOVERNO DA ESTÔNIA. 2024. **Segurança Cibernética**. Disponível em: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>.

GOVERNO DE MALTA. **Lei da Autoridade de Inovação Digital de Malta**. Disponível em: <https://parlament.mt/media/94210/bill-45-malta-digital-innovation-authority-bill.pdf>.

GOVERNO DE MALTA. **Lei de Arranjos e Serviços de Tecnologia Inovadora**. Disponível em: <https://parlament.mt/media/94207/bill-43-innovative-technology-arrangements-and-services-bill.pdf>.

GOVERNO DE MALTA. **Lei de Ativos Financeiros Virtuais**. Disponível em: <https://parlament.mt/media/94209/bill-44-virtual-financial-assets-bill.pdf>.

GREMBERGEN, Wim van; DE HAES, Steven. **Implementing Information Technology Governance: models, practices, and cases**. IGI Publishing, 2008.

Hileman, G., & Rauchs, M. (2017). 2017 **global blockchain benchmarking study**. SSRN Electronic Journal. doi:10.2139/ssrn.3040224.

Huang, Lingling; Zhao, Chengquiang; Chen, Shijie; Zeng, Liujing. **Blockchain: a promising technology for judicial translation services in cases with foreign elements**. Aslib Journal Information Management. Vol. 76 No. 5, 2024. Pp. 713-735. DOI 10.1108/AJIM-11-2022-0485.

Holder, S. (2017). **Can the Blockchain Tame Moscow's Wild Politics?** CityLab, 22 December. Disponível em: <https://www.citylab.com/life/2017/12/can-the-blockchain-tame-moscows-wild-politics/547973/>.

IDZI, Francis Michael. **Governança digital: análise de componentes chave, modelos de contratos sociais e barreiras para o design de políticas públicas**. 100 fls. 2021. Dissertação (Mestrado em Políticas Públicas). Escola de Políticas Públicas e Governo da Fundação Getúlio Vargas. Brasília, 2021, p. 24. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31436>. Acesso em: 14 out. 2024.

ISTOÉ DINHEIRO. **Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais**. Disponível em: <https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/>. Acesso em: 10 de mai. 2022.

JONATHAN MARGULIES. **A Developer's Guide to Audit Logging**. IEEE Security Privacy, 13 (3):84–86, 2015.

Jordi Cucurull & Jordi Puiggalí. **Distributed Immutabilization of Secure Logs**. In: Barthe, G., Markatos, E., & Samarati, P. (eds.). Security and Trust Management, Cham, 2016, pp. 122–137.

JUNIOR, Olavo Brasil de Lima. **As Reformas Administrativas no Brasil: modelos, sucessos e fracassos**. São Paulo: Revista do Serviço Público, 1998.

LAMY, Ana Carolina Faraco; LAMY, Eduardo de Avelar. **Compliance Empresarial**. 1º Edição, Rio de Janeiro: Forense, 2022.

LAGO, Lucas. **Blockchain: confiança através de algoritmos**. Escola Politécnica do Estado de São Paulo, CEST – Boletim, v. 2, n. 4. out. 2017. p. 1.

LEITE, Eduardo de Oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001. p. 22-26.

LING, L. (2019). **Deconstruction of Blockchain**, Tsinghua University Publishing House, Beijing.

LOPES, Marcus Vinícius Pimenta. **A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de provas digitais**. Tese de Doutorado. 218 f. Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023.

Miller, M. 2020. **Bitland: Property Rights for The World's Poor. The Borgen Project**. Disponível em: <https://borgenproject.org/property-rights-for-the-worlds-poor/>

MINISTÉRIO DA ECONOMIA. **Brasil é reconhecido pelo Banco Mundial como o 7º líder em Governo Digital entre 198 países**. Disponível em: <https://www.gov.br/governodigital/pt-br/noticias/brasil-e-reconhecido-pelo-banco-mundial-como-o-7o-lider-em-governo-digital-entre-198-paises>. Acesso em: 09 de nov. 2023.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 14 mai. 2024.

NOHARA, Irene. **Desafios de Inovação na Administração Pública contemporânea: “destruição criadora” ou “inovação destruidora” do Direito Administrativo?** Direito Administrativo. 22/04/2020. Disponível em: <https://direitoadm.com.br/desafios-de-inovacaona-administracao-publica-contemporanea-destruicao-criadora-ou-inovacao-destruidora-dodireito-administrativo/>. Acesso em: 20 set. 2024.

OCDE. **Government at a Glance: Latin America and the Caribbean 2017**. Paris: OECD Publishing, 2016.

PARTH, Thakkar; Senthil, Nathan; Viswanathan, Balaji. **Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform**. In: IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, pages 264–276, 2018.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica: teoria e prática**. 14 ed. ver., atual. e ampl. Florianópolis: Empório Modara, 2018. p. 41, 58, 69, 112-113, 114, 217.

PELOTRA, Mark A. **Blockchain and smart contracts: Legal implications and challenges**. Journal of Law and Technology, 2020.

PIRES, Tatieures Gomes. **Uma avaliação da implantação da Política de Governança Digital na Universidade Federal do Ceará**. 208 fls. 2019. Dissertação (Mestrado Profissional). Programa de Pós-graduação Profissional em Avaliação de Políticas Públicas da Universidade Federal do Ceará. Fortaleza, 2019, p. 79. Disponível em: https://repositorio.ufc.br/bitstream/riufc/49953/3/2019_dis_tgpires.pdf. Acesso em: 13 out. 2024.

PODER JUDICIÁRIO DE SANTA CATARINA. **Missão e Visão**. Disponível em: <https://www.tjsc.jus.br/missao-e-visao>. Acesso em: 21 out. 2024.

PARTH, Thakkar; Senthil, Nathan; Viswanathan, Balaji. **Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform**. In: IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, pages 264–276, 2018.

ROBICHEZ, G. et al. **Blockchain para governos e serviços públicos**. Rio de Janeiro: PUC, 2019. Disponível em: https://www.researchgate.net/profile/Paulo-Henrique-Alves-2/publication/331651536_Blockchain_para_Governo_e_Servicos_Publicos/links/5c86e704458515b59e452f93/Blockchain-para-Governo-e-Servicos-Publicos.pdf. Acesso em: 16 mai. 2024.

RODRIGUES, Mariane Pires. **Governança Digital e transparência pública: uma análise das prefeituras paranaenses**. 183 fls. 2016. Dissertação (Mestrado em Ciência Política). Programa de Pós-Graduação em Ciência Política, Setor de Ciências Humanas, Letras e Artes, Universidade Federal do Paraná. Curitiba, 2016. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/45907/R%20-%20D%20>

%20MIRIANE%20PIRES%20RODRIGUES.pdf?sequence=1&isAllowed=y. Acesso em: 06 out. 2024.

ROSA, Alexandre de Moraes; GARCIA, Lara Rocha; PINTO, Felipe Chiarello de Souza. **Direito para Humanos Robotizados ou Direito dos Robôs Humanizados?** REVISTA NOVOS ESTUDOS JURÍDICOS -ELETRÔNICA, VOL. 28 -N. 3. Disponível em: <https://periodicos.univali.br/index.php/nej/article/view/19985/11614>.

ROSA, Gabriela. **Prevenção e resposta a incidentes cibernéticos**. Florianópolis: Ed. UFSC, 2020.

ROSA, Ramila. **Governança dos Sistemas Judiciais do Poder Judiciário de Santa Catarina**. Revista de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | Salvador | v. 4 | n. 1 | p. 72 – 91 | Jan/Jun. 2018.

SALKIN, Ceren; ONER, Mahir; USTUNDAG, Alp; CEVIKCAN, Emre. **A Conceptual Framework for Industry 4.0**. In: USTUNDAG, Alp; CEVIKCA, Emre (org.). Industry 4.0: Managing The Digital Transformation. Cham: Springer International Publishing, 2018. DOI: 10.1007/978-3-319-57870-5_1. Disponível em: http://link.springer.com/10.1007/978-3-319-57870-5_1. Acesso em: 09 mai. 2024.

SANTOS, Matheus Henrique de Souza. **Aspectos da governança digital na administração pública federal do Brasil sob a luz das orientações da OCDE**. Revista Tempo do Mundo, n. 25, 331-355, abr. 2021. Disponível em: <https://www.ipea.gov.br/revistas/index.php/rtm/article/view/279>. Acesso em: 20 out. 2024.

SANTOS, Roberval de Jesus Leone dos. **Rede Governo: o Portal de Serviços e Informações para o Cidadão**. Relato de experiência. Iniciativa premiada no 7º Concurso Inovação na Gestão Pública Federal. Prêmio Hélio Beltrão – 2002. Disponível em: https://repositorio.enap.gov.br/bitstream/1/554/1/050_02.pdf. Acesso em: 19 out. 2024.

SECRETARIA DE GOVERNO DIGITAL. **Relatório de Resultados 2021**. Brasília: Ministério da Economia, 2021. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/secretaria-de-governo-digital>. Acesso em: 21 maio 2024.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1a ed. São Paulo: Edipro, 2016.

SECHI, Leonardo. **Análise de políticas públicas: diagnósticos de problemas, recomendações de soluções**. São Paulo: Cengage Learning, 2019.

SENADO NOTÍCIAS. **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>. Acesso em: 10 de mai. 2022.

SZABO, Nick. **Smart Contracts: Building Blocks for Digital Markets**. 1996.

Disponível em:

http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT_winterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Acesso em: 19 out. 2024.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Comunicado da Presidência do STJ**.

Disponível em:

<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em: 10 de mai. 2022.

TJSC – Tribunal de Justiça de Santa Catarina. **Resolução nº 17/2021**. Disponível em: <https://www.tjsc.jus.br/documents/37870/5647413/Resolucao+Conjunta+GP-CGJ+n.+17-2021.pdf/12c07e35-554e-5512-17e0-3c5967db6458?t=1624485198145>. Acesso em: 16 mai. 2024.

TJSC – Tribunal de Justiça de Santa Catarina. **Resolução nº 31/2018**. Disponível em:

<http://busca.tjsc.jus.br/buscatextual/integra.do?cdSistema=1&cdDocumento=176659&cdCategoria=1&q=&frase=&excluir=&qualquer=&prox1=&prox2=&prox3=>. Acesso em: 16 mai. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL. CGJ

regulamenta escritura pública de imóveis por token/criptoativo. Disponível em: <https://www.tjrs.jus.br/novo/noticia/cgj-regulamenta-escritura-publica-de-imoveis-por-token-criptoativo/>. Acesso em: 20 out. 2024.

TRIBUNAL SUPERIOR ELEITORAL. **TSE institui comissão presidida por Alexandre e Moraes para acompanhar investigações sobre ação de hackers contra o processo eleitoral**. Disponível em:

<https://www.tse.jus.br/imprensa/noticias-tse/2020/Novembro/tse-institui-comissao-presidida-por-alexandre-de-moraes-para-acompanhar-investigacoes-sobre-acao-de-hackers-contra-o-processo-eleitoral?SearchableText=HACKER>. Acesso em: 05 de mai. 2023.

TAVARES, André Afonso; BITENCOURT, Caroline Müller. **A Lei do Governo Digital e os Laboratórios de Inovação: Inteligência Artificial, Ciência de Dados e Big Open Data como ferramentas de apoio à Auditoria Social e Controle Social**. In: MOTTA, Fabrício; VALLE, Vanice Regina Lírio do. (Coords). *Governo Digital e a busca por inovação na Administração Pública: a Lei n. 14.129, de 29 de março de 2021*. Belo Horizonte: Fórum, 2022.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World**. Penguin, 2016.

THE JAPAN TIMES. (2015). **“Translation firm leaked classified document, NRA says”**. Disponível em:

<https://www.japantimes.co.jp/news/2015/04/01/national/translation-firm-leaked-classified-nradocument-onto-internet-secretariat/>. Acesso em: 20 Mai. 2024.

THE SUPREME PEOPLE'S COURT. **The Supreme People's Court promulgated the Internet court regulations**, *China Information Security*, 2018, pp. 9:30-33.

TORONTO, D., et al. **Blockchain and its impact on legal practices**. *Journal of Law and Technology*, 2021.

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT. (2015). **United States v. Lizarraga-Tirado**, 789 F.3d 1107 (9th Cir. 2015). Disponível em: <https://casetext.com/case/united-states-v-lizarraga-tirado>.

UNIÃO EUROPEIA. CEDH de 04 de novembro de 1950. **Convenção Europeia dos Direitos do Homem**. Roma. 1950.

UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. *Jornal Oficial da União Europeia*, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 26 Set 2023.

VALLE, Vivian Cristina Lima López; GALLO, William Ivan. **Inteligência artificial e capacidades regulatórias do Estado no ambiente da administração pública digital**. A&C – Revista de Direito Administrativo e Constitucional. Belo Horizonte, ano 20, n. 82, pp. 67-86, out./dez. 2020. Disponível em: https://www.academia.edu/47798775/Intelig%C3%A2ncia_artificial_e_capacidades_regulat%C3%B3rias_do_Estado_no_ambiente_da_administra%C3%A7%C3%A3o_p%C3%BAblica_digital. Acesso em: 24 jul. 2024.

VAINZOF, Rony. **Relatório de impacto à proteção de dados pessoais**. In: Renato Opice Blum. (Org.). *Proteção de Dados - Desafios e Soluções na Adequação à Lei*. 1ed. Rio de Janeiro: Forense, 2020, v. 1, p. 141-168.

VIANNA, Bernardo. **Digitalização do setor público é crucial para o desenvolvimento sustentável**. Notícias. Insper. 13/04/2022. Disponível em: <https://www.insper.edu.br/noticias/digitalizacao-do-setor-publico-e-crucial-para-odesenvolvimentosustentavel/#:~:text=O%20C3%8Dndice%20de%20Desenvolvimento%20em,servi%C3%A7os%20p%C3%BAblicos%20por%20meios%20digitais>. Acesso em: 22 set. 2024.

WORLD BANK. 2013. **How Africa Can Transform Land Tenure, Revolutionize Agriculture, and End Poverty**. Disponível em: <https://www.worldbank.org/en/news/press-release/2013/07/22/howafrica-can-transform-land-tenure-revolutionize-agriculture-end-poverty>

ZENG, Liujing; ZHU, Liming; GRAMOLI, Vincent; PONOMAREV, Alexander; SHIPING, Chen. **The Blockchain as a Software Connector**. In: 13th Working IEEE/IFIP Conference on Software Architecture, pages 182–191, 2016.

ZIONTS, J. (2018). “**Blockchain Democracy**” and the Misleading Promise of **Moscow’s Active Citizen Program**. Disponível em: <https://media.consensys.net/blockchaindemocracy-and-the-misleading-promise-of-moscows-active-citizen-program-2eda7141c5b9>. Acesso em: 20 Ago. 2024.

ZOU, J.; YU, B.; ZHUANG, P.; XING, C. (2018). **Blockchain: Core Technologies and Applications**. China Machine Press, Beijing.