INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA

MESTRADO PROFISSIONAL EM DIREITO, JUSTIÇA E DESENVOLVIMENTO

ENTRE SOBERANIA E SUBSERVIÊNCIA DIGITAL

uma análise dos riscos do uso da computação em nuvem no backup dos acervos cartoriais em Pernambuco

Layla Isabelle Sampaio de Carvalho Leite

Dr. Victor Marcel Pinheiro

SÃO PAULO

2024

LAYLA ISABELLE SAMPAIO DE CARVALHO LEITE

ENTRE SOBERANIA E SUBSERVIÊNCIA DIGITAL

uma análise dos riscos do uso da computação em nuvem no backup dos acervos cartoriais em Pernambuco

Defesa de Dissertação de Mestrado desenvolvida sob a orientação do professor Dr. Victor Marcel Pinheiro apresentada para obtenção do título de Mestra pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa –IDP.

Orientador: Dr. Victor Marcel Pinheiro

SÃO PAULO

2024

Código de catalogação na publicação – CIP

L533e Leite, Layla Isabelle Sampaio de Carvalho

Entre soberania e subserviência digital: uma análise dos riscos do uso da computação em nuvem no backup dos acervos cartoriais em Pernambuco / Layla Isabelle Sampaio de Carvalho Leite. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2024.

85 f. il.: color.

Orientador: Prof. Dr. Victor Marcel Pinheiro.

Dissertação (Mestrado Profissional em Direito, Justiça e Desenvolvimento) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Segurança da informação. 2. Computação em nuvem. 3. Acervos cartoriais. I.Título.

CDDir 341.2738

Elaborada por Pollyana da Silva Marra – CRB 1/3704

LAYLA ISABELLE SAMPAIO DE CARVALHO LEITE

ENTRE SOBERANIA E SUBSERVIÊNCIA DIGITA: uma análise dos riscos do uso da computação em nuvem no backup dos acervos cartoriais em Pernambuco

Defesa da Dissertação de Mestrado desenvolvida sob a orientação do professor Dr. Victor Marcel Pinheiro apresentada para obtenção do título de Mestra pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa –IDP.

São Paulo, 18/12/2024

BANCA EXAMINADORA

_____

Victor Marcel Pinheiro

Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa –IDP.

_____

Rafael Silveira e Silva

Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa –IDP.

_____

Carolina Valença Ferraz

Universidade Católica de Pernambuco

]

Dedico esta dissertação à minha bisavó, Dona Senhora, que, no início do século XX, no sertão de Pernambuco, a despeito das proibições do marido, contratou clandestinamente uma professora para alfabetizar todas as suas filhas (incluindo a minha avó paterna). O título de Mestra é um eco de sua coragem revolucionária na crença da educação como ferramenta de libertação, autonomia e autodeterminação.

AGRADECIMENTOS

Desde que eu existo, tenho o privilégio de saber o que é receber o amor incondicional dos meus pais Geovany e Ivone. Sou grata porque fui criada para florescer no que minha alma veio realizar nesta vida. Eles sempre me regaram, nutriram e cuidaram – da menina que amava historinhas e livros de fábulas, a adolescente indignada que os direitos fundamentais não constavam na grade obrigatória do currículo escolar, até a adulta que escolheu fazer do direito à dignidade humana sua trincheira.

Ihering estava certo: é na luta que se finca qualquer esperança de paz dentro desse capitalismo filhote da violência colonial. A história do direito é resistência, é combate, é o escudo dos que recusam se dobrar ao avanço predatório do poder.

E como a luta é coletiva, essa conquista só foi possível graças ao imenso apoio e amor da minha família e amigos. Em nenhum momento ouvi que não seria capaz; pelo contrário, recebi apenas palavras e gestos de encorajamento, que foram fundamentais para chegar até aqui. Agradeço, em especial, a: Alvina, André Felipe, Artemísia, Carolina, Catharine, Dyego, Elisa, Flávia, Júlia, Levy, Lígia, Lucas, Lucia e Matheus. Também a todos que conheci na Casa 1 (Centro de Cultura e Acolhimento LGBT) que transformaram São Paulo na minha casa, o meu lar fora de Pernambuco. Existe amor em SP, pelo menos nas ladeiras do Bixiga.

Aos doutores Antônio e Karem, por cuidarem da minha saúde mental e acolherem as minhas angústias/inquietudes com compaixão e gentileza.

A registradora e tabeliã Ivone Sampaio, pois sem ela a pesquisa não teria sido possível.

Por fim, meu agradecimento ao historiador/escritor/comunicador/professor Jones Manoel, que, em 13 de outubro de 2021, publicou o vídeo “Redes sociais, geopolítica e poder”, o qual foi a inspiração inicial para esta dissertação.

RESUMO

Este trabalho busca identificar, via pesquisa quantitativa, quais são os serviços de computação em nuvem mais utilizados pelos cartórios extrajudiciais em Pernambuco para realizar o procedimento de backup diário do acervo documental, conforme prescreve o Provimento nº 74/2018 da Corregedoria Nacional de Justiça; bem como desenvolver um plano de trabalho para a criação de um Catálogo de Serviços de Nuvem em conformidade com parâmetros de segurança. A pesquisa adota as teorias de colonialismo de dados, soberania de dados, normas de padrão internacional de segurança da informação e princípios de cibersegurança como referencial teórico. Os resultados indicam que, do grupo de amostragem o fornecedor mais utilizado é a Microsoft, mas que existe aderência a empresas nacionais e, por vezes, um uso combinado. Conclui-se que o maior banco de dados pessoais do Poder Público, que são os cartórios extrajudiciais, estão pulverizados em empresas internacionais através do backup atualizado em tempo real; mas é possível mitigar os danos, através de suporte técnico aos cartórios extrajudiciais, recomendações de nuvens devidamente aprovadas pelo Conselho Nacional de Justiça e, de forma macro, a criação de uma infraestrutura nacional que consiga proteger a soberania nacional.

Palavras-chave: Cartório extrajudicial; Provimento nº 74/2018 CNJ; Computação em nuvem; Soberania Digital; Colonialismo de Dados.

ABSTRACT

This study aims to identify, through quantitative research, the most widely used cloud computing services by extrajudicial notary offices in Pernambuco for performing the daily backup procedure of their documentary archives, as required by Provision No. 74/2018 of the National Justice Council. Additionally, it seeks to develop a work plan for creating a Cloud Services Catalog in compliance with security standards. The research adopts data colonialism, data sovereignty, international information security standards, and cybersecurity principles as its theoretical framework. The results indicate that, within the sample group, Microsoft is the most widely used provider, although there is adherence to national companies and, in some cases, a combined use of different providers. It is concluded that the largest repository of personal data under public authority, represented by extrajudicial notary offices, is dispersed across international companies through real-time backup updates. However, it is possible to mitigate risks by providing technical support to extrajudicial notary offices, recommending cloud services previously approved by the National Justice Council, and, on a broader scale, developing a national infrastructure capable of ensuring data sovereignty.

Keywords: Extrajudicial notaries; CNJ Provision No. 74/2018; Cloud computing; Digital sovereignty; Data colonialism.

LISTA DE GRÁFICOS

I Gráfico 6 – Níveis de conectividade significativa e a dimensão territorial no Brasil – 2023.....24
II Figura 3 – Incidência da população com nível mais alto de conectividade significativa (score entre 7 e 9 pontos), por UF (2023).....25
III Qual é o seu município de atuação? 54
IV O seu cartório se localiza na sede da comarca?.....55
V Qual é a atribuição do seu cartório?.....55
VI Identifique o(s) serviço(s) de cloud computing (nuvem) utilizado(s) no cartório para realizar o backup do acervo digital 56
VII Existe um Centro de Processamento de Dados (CPD) isolado no seu cartório?.....57
VIII - Você utiliza a versão corporativa/paga?.....58
IX O servidor da nuvem utilizado está localizado no Brasil? 59

LISTA DE TABELAS

1 Características da computação nas nuvens. 34
2 Resumo da Metodologia – Pesquisa Documental 41
3 Resumo da Metodologia – Pesquisa Quantitativa 53

LISTA DE SIGLAS E ABREVIATURAS

ABDI – Agência Brasileira de Desenvolvimento Industrial

ANPD – Autoridade Nacional de Proteção de Dados Pessoais

ARPANET – Advanced Research Projects Agency Network

AWS – Amazon Web Services

CENSEC – Central Eletrônica Notarial de Serviços Compartilhados

CGJ-PE – Corregedoria Geral da Justiça de Pernambuco

CIA - Central Intelligence Agency

CISCO – Cisco Systems, Inc.

CNJ – Conselho Nacional de Justiça

DNV – Declaração de Nascido Vivo

DOI – Imposto sobre Declaração sobre Operações Imobiliárias

ENIAC – Electronic Numerical Integrator and Computer

ENISA – European Union Agency for Cybersecurity

EU – União Europeia

EUA - Estados Unidos da América

GAFAM – Google (Alphabet), Apple, Facebook (Meta Platforms), Amazon e Microsoft

GCHQ – Government Communications Headquarters

GDPR – General Data Protection Regulation

IBGE - Instituto Brasileiro de Geografia e Estatística

ISSO/IEC – International Organization for Standardization/ International Electrotechnical Commission

LGPD – Lei Geral de Proteção de Dados Pessoais

MDIC – Ministério do Desenvolvimento, Indústria, Comércio e Serviços

NIST – National Institute of Standards and Technology

NSA – National Security Agency

SIM – Sistema de Informações sobre Mortalidade

SINASC – Sistema de Informações sobre Nascidos Vivos

SLAs – Service Level Agreement

TICs – Tecnologias da Informação e da Comunicação

UNIVAC I – UNIVersal Automatic Computer

UPS – Uninterruptible power supply (nobreak)

SUMÁRIO

1 INTRODUÇÃO 15

2 NOVOS DOMÍNIOS, VELHAS PRÁTICAS: O COLONIALISMO DE DADOS EM AMBIENTES DE COMPUTAÇÃO EM NUVEM 19

2.1 Colonialismo Histórico: a invasão que nunca acabou. 19

2.2 Colonialismo Moderno: a exploração atualizada. 20

2.3 A preservação da fortuna colonial e seu papel no financiamento do mundo digital 22

2.3.1 Security & resilience in governmental clouds: uma recomendação da ENISA 26

2.3.2 Espionagem e Ameaças à Soberania Brasileira no Século XXI: a internet nunca foi um território neutro. 27

2.4 Soberania de Dados e Serviços de Computação em Nuvem: O Novo Campo de Batalha Geopolítica 29

3 A INFRAESTRUTURA TANGÍVEL DO TERRITÓRIO DIGITAL 32

3.1 A Base Léxica da Tecnologia da Informação 32

3.1.1 Dados e banco de dados 32

3.1.2 Computação em nuvem 33

3.1.3 Data center 35

3.1.4 Backup 38

3.2 A concentração do poder tecnológico da Microsoft Corporation: pesquisa documental sobre incidentes de segurança cibernética da empresa. 40

3.2.1 Casos de Incidentes de Segurança 41

3.2.1.1 Julho de 2023: Invasão da plataforma de e-mail da Microsoft e roubo de e-mails do Departamento de Estado dos EUA. 42

3.2.1.2 Janeiro de 2024: Hackers russos utilizaram a técnica de "Pulverização de Senhas" para invadir a Microsoft em novembro de 2023 43

3.3 Análise de pesquisas de mercado sobre confiabilidade nos serviços de computação em nuvem 44

4 O USO DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM NOS CARTÓRIOS EXTRAJUDICIAIS DE PERNAMBUCO: PESQUISA E PROJETO DE GOVERNANÇA 46

4.1 A formalidade documental da pessoa natural: A importância da segurança jurídica proporcionada pelos serviços cartorários extrajudiciais 46

4.1.1 A qualidade do banco de dados 49

4.2 O Provimento nº 74 de 31/07/2018 50

4.3.1 Metodologia 52

4.3.2 Análise dos dados coletados 53

4.3.2.1 Municípios de atuação 53

4.3.2.2 Localização do cartório na sede da comarca 54

4.3.2.3 Atribuição dos cartórios extrajudiciais 55

4.3.2.4 e 5 Serviços de computação em nuvem 55
4.3.2.6 Centro de Processamento de Dados (CPD) 57
4.3.2.7 Utilização de versão corporativa/paga 58
4.3.2.8 Localização do Servidor de Nuvem 58
4.3 Arcabouço Jurídico 59
4.3.1 Constituição Federal 59
4.3.2 Lei dos Cartórios 60
4.3.3 Regimento Interno do Conselho Nacional de Justiça 60
4.3.4 Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco 61
4.4 Projeto de Governança: Catálogo de Serviços de Nuvem em conformidade com parâmetros de segurança 61
4.4.1 1ª Etapa: Mapeamento extensivo dos provedores contratados 62
4.4.2 2ª Etapa: Inventário da Documentação e Classificação 62
4.4.3 3ª Etapa: Teste de Segurança da Informação 63
4.4.4 4ª Etapa: Ranqueamento 63
4.4.4.5 Ecossistema próprio 64
CONCLUSÃO 65
REFERÊNCIAS 67
APÊNDICE B – Formulário da Pesquisa 80
ANEXO – Anexo IV Completo "Security & Resilience in Governmental Clouds" 83

1 INTRODUÇÃO

O Provimento nº 74/2018, que regula "os padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil" foi publicado pelo Conselho Nacional de Justiça em um esforço coordenado para integrar a base de dados dos cartórios extrajudiciais com segurança e nivelamento de possibilidades, dentro das realidades de cada unidade.

O *framework* delineado segue padrões internacionais de boas práticas e é muito eficiente tanto quanto medida preventiva para possíveis incidentes de segurança, como para gestão de crise. Além da cópia física, a cópia de segurança do acervo deve ser diariamente alimentada e arquivada em caráter de backup nos serviços de computação em nuvem. Essa diretriz segue a máxima da segurança da informação de "quem tem um backup não tem nenhum e que tem dois, tem um", em virtude da facilidade de perda, corrupção do arquivo, invasão dos dispositivos etc.

A nuvem foi uma revolução nas possibilidades da capacidade de tratamento de dados, pois liberou espaço na máquina para que o sistema operacional rode com maior fluidez, criou a disponibilidade imediata dos arquivos, em qualquer momento e a qualquer hora apenas necessitando de conexão de internet. Os computadores domésticos e empresariais não suportavam mais a produção diária de arquivos.

A escolha de qual provedor do serviço de computação em nuvem a ser contratado está a critério do delegatário responsável pelo cartório extrajudicial, que certamente leva em consideração o valor da arrecadação semestral e, inevitavelmente, o volume da documentação produzida. A discricionariedade deve sempre ser respeitada, porém, é possível inquirir se a ausência de orientações é o melhor caminho a ser adotado.

Até o momento não existe uma lista homologada que indique os fornecedores aprovados pelo Conselho Nacional de Justiça ou que certifique quais são os mais seguros para o armazenamento do banco de dados. Em virtude dessa lacuna, as cópias de segurança dos mais de 15 mil cartórios extrajudiciais do país estão pulverizadas em diversas empresas, algumas nacionais, mas, em sua maioria, internacionais do Norte Global.

As chamadas "*big techs*" são as grandes corporações estadunidenses do acrônimo GAFAM: Google (agora Alphabet Inc), Apple, Facebook (agora Meta Platforms, Inc), Amazon e Microsoft que possuem o oligopólio do mercado ocidental de tecnologia; sendo assim, ainda que os *data centes* e servidores estejam localizados no território nacional, o maior banco de dados pessoais do povo brasileiro, atualizado em tempo real é entregue para várias empresas

diferentes e de países diferentes. Dados pessoais são informações que identificam ou podem identificar uma pessoa natural e o direito à proteção é garantido tanto pela Lei Geral de Proteção de Dados Pessoais (LGPD) quanto pela Constituição Federal.

A teoria do colonialismo de dados é utilizada como o fio condutor para traçar o caminho percorrido desde a herança da acumulação tradicional de riquezas até a exploração dos dados, que são a nova matéria-prima em exploração, desenhando a relação de desigualdade entre indivíduos e empresas; e, para continuar a jornada, a teoria da soberania de dados e a sua preocupação com o território online e questões geopolíticas será instrumental para a análise da pesquisa realizada.

O contraponto entre colonialismo e soberania no mundo digital e no tratamento de dados pessoais é um tema atual e relevante, sobretudo para que o Brasil possa reger-se pelos princípios constitucionais de independência nacional, autodeterminação dos povos e não-intervenção, superando a condição de consumidor passivo.

Embora o modo de produção colonial tenha sido formalmente abolido, a sua lógica estrutural permanece nas relações internacionais. Isso se evidencia na dinâmica de exportar a matéria-prima (dados) e, em contrapartida, importar o produto final já processado (na infraestrutura tecnológica), reproduzindo assim, no ambiente digital, o padrão colonial de dependência e subordinação.

A Assembleia Constituinte, na construção Constituição Federal da República Federativa do Brasil, elegeu a soberania como o primeiro fundamento descrito e o reiterou com o princípio de independência nacional nas suas relações internacionais. Segundo Ferreira Filho (1990), a soberania é enfatizada na Constituição com o objetivo de destacar a independência do Brasil em relação a qualquer poder estrangeiro, seja de Estados ou organizações internacionais, demonstrando o caráter externo da soberania como não sujeição e independência.

Para proteger a autodeterminação é preciso ter o controle e domínio das próprias informações e ser livre da possibilidade de intervenção na democracia como decorrência da sujeição, bem como a capacidade de se proteger de cenários de guerra, retaliação internacional, desastres ambientais etc. A teoria do colonialismo de dados que a princípio foca nas relações entre pessoas humanas e pessoas jurídicas privadas, será ampliada e utilizada para compreender as novas dinâmicas geopolíticas de soberania.

A pesquisa tem os seguintes objetivos específicos: (i) analisar a dependência tecnológica do Brasil aplicando a teoria do colonialismo de dados, a fim de desenvolver uma leitura crítica do Provimento nº 74/2018 do CNJ; (ii) identificar, via pesquisa quantitativa, quais são os serviços de computação em nuvem mais utilizados pelos cartórios extrajudiciais em Pernambuco para a realização, do backup dos seus acervos, em conformidade com o aludido Provimento (iii) a partir dos resultados consolidados da supracitada, investigar se a empresa mais utilizada é adequada, do ponto de vista de gerenciamento de incidentes de segurança, para armazenar os arquivos do Poder Público, considerando a legislação brasileira e os princípios constitucionais relacionados à independência nacional e à não-intervenção; (iv) desenvolver uma proposta de projeto que possa auxiliar na resolução da problemática.

O segundo capítulo é dedicado à construção da base teórica da dissertação ao apresentar os conceitos-chave e contextualização histórica entre as técnicas de exploração históricas e atuais. Para fazer a discussão sobre os riscos da dependência de provedores estrangeiros são demonstrados os efeitos do colonialismo histórico no colonialismo de dados e cibersegurança, teoria que destaca a concentração de poder informacional por grandes empresas de tecnologia, geralmente sediadas nos EUA ou Europa.

Ademais, também é realizada a análise do estudo "Security & Resilience in Governmental Clouds" da Agência Europeia para a Segurança das Redes e da Informação e um levantamento dos casos de interferência na soberania brasileira através do espaço digital.

O terceiro capítulo se propõe a explicar a infraestrutura tecnológica em debate e detalhar todos os elementos que compõem o serviço de computação em nuvem, proporcionando uma compreensão abrangente do tema. Para aferir a confiabilidade das empresas privadas internacionais é realizada uma pesquisa documental dos relatórios e reportagens dos incidentes de segurança mais recentes da Microsoft Corporation., seguindo aos critérios: o volume e sensibilidade de dados vazados e a gravidade das consequências para os clientes e a própria empresa.

De forma complementar é brevemente analisada a percepção do mercado da iniciativa privada nacional, por meio de pesquisas de benchmark de estudos realizados por empresas especializadas em tecnologia e o Núcleo de Informação e Coordenação do Ponto BR.

O quarto e último capítulo faz o recorte do banco de dados dos cartórios extrajudiciais de registro civil para investigar a importância da proteção dos dados pessoais presentes no

acervo; explora em maiores detalhes as disposições do Provimento nº 74/2018 da CNJ; apresenta os resultados da pesquisa quantitativa e a proposta do projeto de governança.

A pesquisa objetiva identificar, por meio de amostragem, qual é o serviço de nuvem mais utilizado pelos cartórios extrajudiciais de Pernambuco. Para atingir esse propósito, foi utilizada a metodologia quantitativa para coletar, organizar e interpretar os dados apurados via questionário estruturado em formulário online.

Por fim, a partir dos dados interpretados, é desenvolvido um plano de trabalho de estudo diagnóstico-propositivo para catalogar desenvolver um Catálogo de Serviços de Nuvem em conformidade com parâmetros de segurança a ser oferecido aos delegatários, para que possam fazer uma escolha informada.

Diante da interdisciplinariedade e complexidade do tema a ser desenvolvido, o trabalho adota uma abordagem mista de metodologias: bibliográfica, quantitativa e documental. A bibliografia foi formada por livros jurídicos; artigos científicos; normas de padrão internacional de segurança da informação; textos normativos e regulatórios; legislação brasileira e legislação internacional; relatórios e pareceres técnicos emitidos por órgãos reguladores; transcrições de discursos de autoridades; podcasts especializados no tema de computação em nuvem; palestras realizadas em congressos nacionais sobre o tema de soberania; reportagens sobre os casos analisados; conceitos encontrados nos sites das empresas fornecedoras do serviço de computação em nuvem.

Os cartórios desempenham um papel essencial para a segurança do ordenamento jurídico, conforme descrito na Lei nº 8.935/94 (Lei dos cartórios), a organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos, de forma que o seu banco de dados deve ser prioridade.

2 NOVOS DOMÍNIOS, VELHAS PRÁTICAS: O COLONIALISMO DE DADOS EM AMBIENTES DE COMPUTAÇÃO EM NUVEM

2.1 Colonialismo Histórico: a invasão que nunca acabou.

É possível traçar um paralelo entre as antigas metodologias de exploração metrópole-satélite (Portugal – Brasil) e a atual dependência do Sul Global da infraestrutura tecnológica controlada pelo Norte Global, aqui representado pelos Estados Unidos da América.

O longo período da colonização exploratória no Brasil produziu um modelo de sistema econômico capitalista com características particulares, oriundas das profundas raízes forçadamente plantadas na invasão e constante ocupação da América Latina pelos reinos europeus, principalmente por Portugal e Espanha e, de forma indireta, pela Inglaterra, do século XVI ao XIX.

O sistema colonial organizava-se, tanto legal e política, quanto fiscal e financeiramente, para drenar as riquezas de dentro para fora (Fernandes, 2006). Nesse arranjo as regiões produtoras de bens primários foram, uma a uma, estagnando (Frank, 1969), formando o padrão cíclico: rápido progresso econômico e aparente prosperidade, seguido por um declínio vertiginoso no valor das commodities, a exemplo do desmatamento do Pau-Brasil e a produção de açúcar, tabaco e algodão no Nordeste.

Mesmo com a exploração itinerante pelo território nacional, o senhor de engenho tinha um sistema caracterizado por não ser autogerador e nem sustentável. A sua produção era “do tipo colonial, ou seja, uma produção estruturalmente heteronômica, destinada a gerar riquezas para a apropriação colonial” (Fernandes, 2006) por meio da apropriação dos recursos que estavam "apenas ali" para serem tomados por meio da força, violência, fraude e enganações.

Segundo Tavares (2019), entre os escombros do império português e a expansão do império inglês, o Brasil viveu a transação do modelo de extração colonial para a acumulação capitalista interna, majoritariamente na região sudeste. As oligarquias regionais se espalharam pelos territórios e consolidaram o poder político e a capacidade de se abrir ao capital estrangeiro, criando ilhas burguesas no eixo São Paulo-Rio de Janeiro e, posteriormente, no país inteiro. Essa transação aconteceu após o apático processo da Proclamação da República.

Carvalho (2001) aponta que, ao conquistar sua independência, o Brasil herdou não apenas a unidade territorial, linguística, cultural e religiosa deixada pelos portugueses, mas também uma “tradição cívica pouco encorajadora”. A República dos Estados Unidos do Brazil

nasceu com uma população analfabeta, uma sociedade escravocrata, uma economia baseada na monocultura e no latifúndio, e era um Estado de tradição absolutista.

A cultura remanescente do eurocentrismo, que enaltece a civilização europeia como o ápice do desenvolvimento humano, ajudou na perpetuação da desigualdade e sedimentou a crença de que o que vem "de fora" tem qualidade, conforme descrito por Frank (1969),

> Os países que hoje são desenvolvidos nunca foram subdesenvolvidos, embora possam ter sido não desenvolvidos. [...] o subdesenvolvimento contemporâneo é, em grande parte, o produto histórico das relações econômicas e outras, passadas e contínuas, entre os países satélites subdesenvolvidos e os países metropolitanos agora desenvolvidos.

Hoje a capacidade notável do capitalismo de evoluir e adaptar-se para preservar a sua predominância e o *status quo* significa a absorção de novas tecnologias e estruturas, com todas as vantagens comerciais e políticas ao seu favor.

Dadas as devidas proporções (para não incorrer na banalização do genocídio indígena, tráfico humano transatlântico, escravidão e as sérias consequências ambientais, políticas e sociais no mundo todo), o Brasil herdou e manteve a dinâmica de extração da colônia para a metrópole, porém atualizou por meio de um *rebranding*.

2.2 Colonialismo Moderno: a exploração atualizada.

No século XXI a evolução da exploração de recursos foi descrita por Couldry e Mejias (2019) na teoria do "Colonialismo de Dados", que se propõe a analisar as dinâmicas de poder entre as forças diametralmente opostas da proteção da privacidade e a autonomia das pessoas físicas do Sul Global versus o tratamento (como as práticas de coleta, armazenamento, análise e uso) de dados desenfreado e exploratório por grandes corporações e governos, frequentemente situados em países do Norte Global.

Os autores enfatizam que "o colonialismo é sobre apropriação; enquanto o colonialismo histórico apropriava terras, recursos e corpos, o novo colonialismo de hoje se apropria da vida humana ao extrair valor dos dados", portanto não é uma substituição, é uma adição ao *modus operandi*, um novo território.

A base de toda a nova estrutura são os dados pessoais, definidos no art.5º, I da Lei nº 13.709/2018 ou Lei Geral de Proteção de Dados Pessoais (LGPD) como "informação relacionada a pessoa natural identificada ou identificável". É através da invasão da intimidade, rastreamento das pegadas digitais, coleta e interpretação de hábitos sociais, das preferências de

consumo, conteúdos, serviços e produtos, que é possível compreender não apenas o indivíduo, mas grupos inteiros.

O instrumento de captação dos dados pessoais são as plataformas digitais e os muitos produtos e serviços inescapáveis em quase todos os espaços da vida humana, incluindo as interações com família, amigos, parceiros amorosos e colegas de trabalho, os espaços das casas e cidades, hobbies e entretenimentos, exercícios, discussões políticas, registros de saúde, deslocamentos e estudos, criando uma forma de "colonização" digital que dificilmente deixa qualquer área ou atividade intocada (Mejias e Couldry, 2024).

Nesse contexto, o tratamento sistematizado de todas essas informações converte os dados pessoais em commodities digitais intangíveis, ou seja, produto ou recurso que pode ser comprado, vendido ou negociado em um mercado. Esse conceito é especialmente significativo na economia digital, onde vastas quantidades de dados são coletadas, analisadas e utilizadas para diversos fins e com um relativo baixo custo de produção.

A problemática da comodificação da vida humana para a acumulação de capital é agravada quando um país precisa da infraestrutura tecnológica de propriedade de empresas privadas de outro país, que geralmente possuem laços com os seus governos, como acontece com os maiores *players* do mercado de tecnologia, que são as *big techs* estadunidenses, conhecidas pelo acrônimo GAFAM: Google (agora Alphabet Inc.), Apple Inc, Facebook (agora Meta Platforms, Inc.), Amazon.com, Inc e Microsoft Corporation.

Para utilizar os serviços das plataformas digitais é preciso que o usuário aceite os Termos de Uso, um contrato de adesão que raramente é lido, especialmente se for de um serviço necessário ou "*trending*", favorecendo um cenário de entrega forçada dos dados solicitados (o baixo custo de produção) em um padrão de alta rastreabilidade e tratamento dos dados "para a melhoria do serviço", como frequentemente afirmado nos Termos de Uso e Políticas de Privacidade, instrumentos de autorregulação corporativa.

No entanto, práticas que extrapolam essa autorregulação têm sido alvo de escrutínio. A Alphabet Inc. (conglomerado de empresas do Google) foi condenada em agosto de 2024, pelo juiz Amit P. Mehta, em ação movida pelo Departamento de Justiça do governo americano que denunciou as práticas de corrupção e monopólio de exclusão ao criar barreiras para o crescimento dos buscadores concorrentes, como o Bing e DuckDuckGo.

Através de acordos de exclusividade o Google pagou bilhões de dólares ao longo de décadas a empresas como a Apple e Samsung para garantir uma posição privilegiada em dispositivos e navegadores. Essa prática consolidou o navegador e buscador Chrome como o mais utilizado, com receita anual superior a US$ 300 bilhões (trezentos bilhões de dólares americanos) majoritariamente oriunda de anúncios de pesquisa (Bloomberg, 2024).

O caso demorou quatro anos para ser julgado e a decisão será apelada, mas até o momento a situação aparenta ser um passo importante para criação de precedentes combatam as práticas de truste das *big techs*.

Mesmo com a condenação criminal, a Alphabet, holding dona do Google, registrou um lucro líquido de US$ 26,3 bilhões (vinte e seis bilhões e trezentos milhões de dólares americanos) no terceiro trimestre de 2024, um aumento de 33,6% em relação ao mesmo período de 2023. Suas receitas consolidadas aumentaram 15% no comparativo com o ano anterior, alcançando US$ 88,3 bilhões (oitenta e oito bilhões e trezentos milhões de dólares americanos), superando as expectativas do mercado. O presidente-executivo da empresa, Sundar Pichai, afirmou que os investimentos em inteligência artificial (IA) têm se mostrado eficazes, especialmente nos segmentos de pesquisa e serviço de computação em nuvem, com a receita da plataforma de nuvem do Google alcançando US$ 11,35 bilhões (onze bilhões e trezentos e cinquenta milhões de dólares americanos), acima da previsão dos analistas (ISTOÉ DINHEIRO, 2024).

A centralização do processamento de dados no Norte Global perpetua uma distribuição desigual dos benefícios econômicos derivados dessa nova forma de matéria-prima. As ideologias contemporâneas que justificam essa exploração frequentemente retratam a coleta massiva de dados como um avanço inevitável ou como um benefício para a sociedade, ocultando suas raízes exploratórias e as consequências para a autonomia das pessoas e soberania digital das nações exploradas.

Sendo assim, a teoria do colonialismo de dados não procura uma metáfora, apenas identifica a realidade concreta e descreve as mudanças profundas em curso no capitalismo contemporâneo, que redireciona o seu eixo de expansão para o novo material bruto.

2.3 A preservação da fortuna colonial e seu papel no financiamento do mundo digital

Inicialmente o território digital aparentava ter jurisdições borradas em virtude da autorregulação, porque, de fato, a Lei da internet era a linguagem do código programado para

o software (Lessig, 2006). Esse furor da liberdade disruptiva criou o *ethos* que prezava pela privacidade e opacidade dos rastros da presença online, mas as fronteiras foram desenhadas embaixo dos narizes de todo o mundo, pela própria história do espaço digital.

O primeiro computador totalmente funcional do mundo, o *Electronic Numerical Integrator and Computer* (ou *ENIAC*) foi fruto de um projeto financiado pelo governo dos Estados Unidos da América; a construção do dispositivo durou dois anos e custou aproximadamente US$ 400.000 (quatrocentos mil dólares americanos). A função original era calcular tabelas de alcance de artilharia durante a Segunda Guerra Mundial, porém, a máquina não ficou pronta a tempo e a sua inauguração foi em novembro de 1945, dois meses após o fim da guerra. A máquina foi reutilizada para a realização de diversas outras aplicações e cálculos para o desenvolvimento de armas nucleares (História dos Computadores, 2024).

Apenas em fevereiro de 1946 o ENIAC foi revelado ao público como uma "máquina matemática" capaz de revolucionar o campo da engenharia e mudar os métodos de design industrial. A apresentação sublinhou a capacidade da máquina de "libertar o pensamento científico do trabalho árduo de cálculos longos" (Smithsonian Magazine, 2024).

O projeto foi uma parceria entre o governo estadunidense e o "*Moore School of Electrical Engineering at the University of Pennsylvania*" (Departamento de Engenharia Elétrica e de Sistemas). Somente após o sucesso do ENIAC que empresas privadas começaram a investir no produto e transicionar para o setor privado, como a Remington Rand que criou o primeiro computador comercial, o *UNIVAC I (UNIVersal Automatic Computer)*, que também era utilizado pelo governo estadunidense.

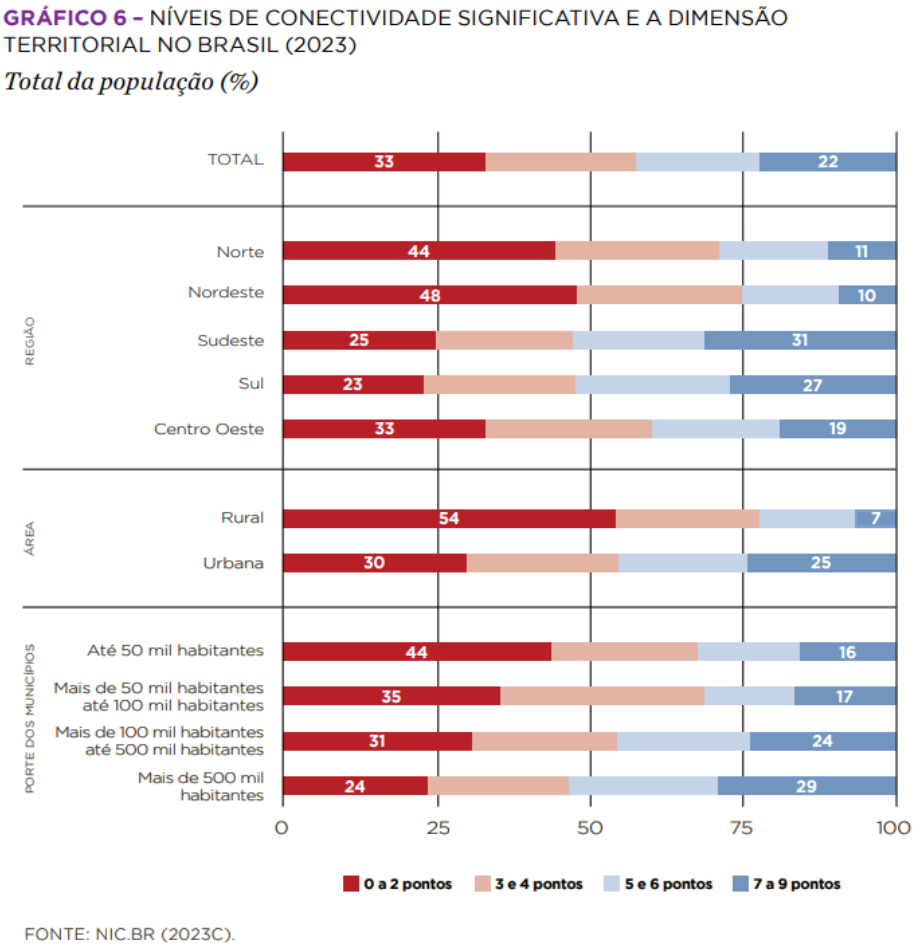
Os computadores foram criados e comercializados, mas ainda não tinham atingido seu total potencial. O que hoje é a "internet" foi um projeto (Advanced Research Projects Agency Network – ARPANET) desenvolvido durante a Guerra Fria, também pelo governo dos Estados Unidos da América, como ferramenta de inteligência de guerra.

O propósito da primeira rede de computadores era integrar os centros científicos de pesquisa espalhados pelo país para criar um caminho comum de transmissão de informações militares sigilosas. Existia a necessidade de alinhar as estratégias e resistir a possíveis ataques à rede, especialmente um ataque nuclear. Toda a informação governamental sigilosa que trafegou durante a Guerra Fria estava segura e protegida dentro do país.

Vários países se interessaram pela tecnologia e a difusão ocorreu, simultaneamente durante a década de 1990, tanto na Europa Ocidental quanto no Brasil, sendo a maior diferença a velocidade da expansão e qualidade do serviço. A fortuna colonial proporcionou que o continente europeu tivesse melhores infraestruturas de telecomunicações e investimentos públicos e privados no setor, garantindo uma vantagem.

A situação nacional ainda é de significativa deficiência, conforme a pesquisa de 2023 "Conectividade Significativa: propostas para medição e o retrato da população no Brasil", que em sua metodologia multifatorial considera "Os níveis de conectividade significativa serão analisados pelas seguintes variáveis: (a) regiões do país, (b) áreas (rurais e urbanas) e (c) porte dos municípios, a partir do tamanho da população" e a proporcionalidade entre a relação do tamanho populacional e a conectividade.

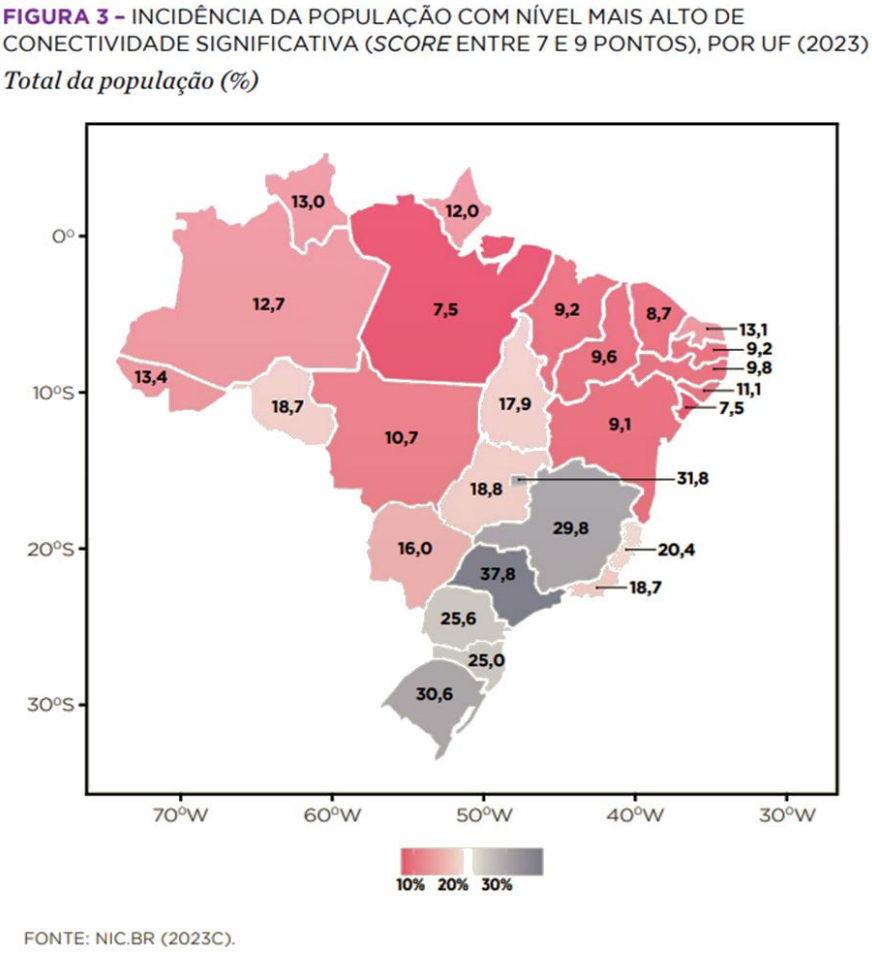
I Gráfico 6 – Níveis de conectividade significativa e a dimensão territorial no Brasil – 2023



Fonte: CGI.br, 2024

A desigualdade no acesso à internet está diretamente relacionada à infraestrutura de conexão disponível em determinada região, sendo que áreas de menor renda tendem a enfrentar mais dificuldades nesse aspecto. Como a banda larga fixa é contratada com base na velocidade de tráfego e a banda larga móvel pela quantidade de dados consumidos, usuários de menor poder aquisitivo, que predominantemente utilizam a internet móvel, acabam enfrentando restrições no acesso a conteúdo online, o que contribui para a ampliação das desigualdades digitais.

II Figura 3 – Incidência da população com nível mais alto de conectividade significativa (score entre 7 e 9 pontos), por UF (2023)



Fonte: CGI.br, 2024

Os estados do Norte e Nordeste, que apresentam os piores índices, também concentram os municípios com maior vulnerabilidade social, considerando infraestrutura urbana, capital humano e renda. Mesmo no Sudeste e Sul, regiões com melhor desempenho, há disparidades internas relevantes. São Paulo, com a maior economia do país e responsável por 30,2% do PIB nacional em 2021, lidera em conectividade significativa, mas ainda enfrenta barreiras para garantir acesso adequado a toda a população (CETIC.BR, 2024).

2.3.1 Security & resilience in governmental clouds: uma recomendação da ENISA

A proteção de dados na União Europeia (EU) passou por importantes mudanças ao longo do tempo. Em 1995 o Parlamento Europeu e do Conselho da UE publicou a Diretiva 95/46/CE "relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", um dos documentos mais importantes para a temática de fluxo de dados e compartilhamento entre países. O documento foi revogado e substituído em 2016 pelo Regulação (EU) 2016/679 (General Data Protection Regulation – GDPR).

A Diretiva foi vanguardista ao estabelecer que a proteção não deveria ser comprometida, mesmo quando o responsável pelo tratamento estivesse fora da União Europeia; que a legislação aplicável seria a do Estado-Membro onde os meios de tratamento estão localizados, garantindo que os direitos dos titulares sejam respeitados e as obrigações dos responsáveis cumpridas; e, por fim, ao abordar a integração econômica-social e aumento dos fluxos transfronteiriços de dados, pormenorizando os mecanismos para que a localização do responsável pelo tratamento não comprometa os direitos dos titulares ou resulte em desvio de informações entre os países.

Cinco anos antes do GDPR, em 2011, a Agência Europeia para a Segurança das Redes e da Informação (ENISA) publicou o Relatório "*Security & Resilience in Governmental Clouds*", a segunda versão de um estudo iniciado em 2009.

O Relatório de 2011 se propõe a dar suporte técnico para os governos dos Estados-Membros da União Europeia tomarem decisões informadas sobre a escolha do modelo dos serviços de computação em nuvem. O pressuposto inicial era a necessidade de avaliar o papel da computação em nuvem na proteção de infraestruturas críticas de informação, destacando que, "em um futuro próximo", essa tecnologia atenderia uma parte significativa dos cidadãos da União Europeia, empresas e administrações públicas.

De forma muito objetiva também ressalta a indispensabilidade de uma organização da estratégia nacional que considere os efeitos da interoperabilidade entre nuvens nacionais e supranacionais, o impacto de falhas em cascata, a inclusão dos provedores de nuvem em esquemas de *report* existentes e a preparação para a gestão de crises em incidentes de grande escala. As instruções para análise da rede de computação em nuvem se encontram no Anexo III

e a descrição de todas as possíveis ameaças estão descritas na extensa lista do Anexo IV, que é particularmente importante para compreender o porquê das recomendações.

O Anexo IV (ver Anexo) do relatório lista quarenta e nove ameaças à segurança da informação, entre elas estão o acesso não autorizado às instalações (inclusive físico), roubo de backups, perda de chaves de criptografia, exclusão insegura de dados, perda de governança e controle devido a SLAs incompletos, falência ou aquisição de provedores de nuvem (o que pode comprometer acordos e gerar mudanças estratégicas), além de responsabilidades legais e regulatórias, como a notificação de violações de segurança. Outras questões incluem conflitos entre exigências de privacidade e segurança, bem como diretrizes regionais incompatíveis.

Em síntese, o mapeamento que a ENISA publicou em 2011 já apontava a seriedade e urgência do tópico, antes mesmo de escândalos internacionais trazerem as questões de segurança governamental para o debate público ou até da adoção massiva do uso da nuvem como praxe para armazenamento de dados, tanto privados quanto públicos.

2.3.2 Espionagem e Ameaças à Soberania Brasileira no Século XXI: a internet nunca foi um território neutro.

Edward Snowden, ex-administrador de sistemas da Central Intelligence Agency – CIA e ex-analista da National Security Agency – NSA, através da matéria "The NSA Files" no jornal The Guardian em 2013, expôs as práticas de monitoramento dos cidadãos norte-americanos e espionagem em outros países. O então presidente Barack Obama justificou o procedimento como protocolo para ações antiterroristas.

Uma das técnicas era o perfilamento de uma pessoa através do monitoramento dos metadados, os dados que informam as características da informação-dado. À época a NSA arguiu que metadados não são dados pessoais e, portanto, não violam a privacidade de ninguém; os ativistas reiteraram que os metadados não são informações identificadas, mas que podem ser identificáveis após tratamento.

O Brasil e a ex-presidenta Dilma Rousseff estavam listados como alvo da espionagem. Houve o monitoramento das embaixadas brasileiras, das ligações da então presidenta e monitoramento do funcionamento da empresa Petrobrás, que, segundo a BBC (2013), o interesse dos americanos estaria relacionado à tecnologia brasileira envolvida na exploração em águas profundas da camada do pré-sal brasileiro.

A retaliação diplomática foi significativa e, o durante a 68ª Assembleia-Geral das Nações Unidas, a Dilma Rousseff falou que a situação no Brasil foi especialmente grave, diante das intrusões que resultaram na interceptação indiscriminada de dados pessoais de cidadãos, informações empresariais de alto valor econômico e estratégico, além de comunicações de representações diplomáticas, incluindo a Missão Permanente junto às Nações Unidas e a Presidência da República. Também destacou a urgência de estabelecer condições para que o espaço cibernético não seja utilizado como arma de guerra, através de espionagem, sabotagem e ataques contra sistemas e infraestrutura de outros países.

Seria injusto, diante da configuração socioeconômica do nosso capitalismo dependente, exigir do Brasil o mesmo nível de investimento em tecnologia que os Estados Unidos da América ou a Inglaterra foram capazes de realizar. Em um dos mais de 50 mil documentos fornecidos por Edward Snowden ao jornal The Guardian em 2013 na reportagem "NSA files decoded", veio a público o caso da parceria entre as agências de inteligência dos Estados Unidos (NSA) e do Reino Unido (GCHQ) para a interceptação de cabos de fibra ótica para coletar quantidades massivas de dados como e-mails, mensagem de texto, histórico de navegação, metadados de ligações telefônicas e tráfego online em escala global, por meio de acesso aos cabos de fibra ótica com a técnica de exploração de fontes especiais.

Além da interceptação e extração dos dados, também houve a invasão de protocolos de segurança online, incluindo criptografia usada por serviços populares como Google, Facebook e Yahoo, conforme reportado pela BBC (2013):

> Os serviços de inteligência de EUA e Grã-Bretanha teriam quebrado a tecnologia usada para criptografar serviços de internet, tais como serviços bancários online, registros médicos e e-mails (...) se concentrando na criptografia usada em smartphones, e-mail, compras online e redes de comunicação remota para negócios.

A NSA também teria colaborado com empresas de tecnologia - não nomeadas - para construir as chamadas "portas dos fundos" de softwares produzidos por estas companhias, o que daria ao governo acesso a informações do usuário antes que estas sejam criptografadas e enviadas pela internet. Na década seguinte, a NSA teria empregado computadores de quebra de código e começado a colaborar com as empresas de tecnologia americanas e no exterior para construir pontos de acesso a seus produtos.

Para invadir computadores e capturar mensagens antes de serem criptografadas, a NSA teria utilizado ampla influência para introduzir fraquezas em padrões de criptografia usados pelos desenvolvedores de software em todo o mundo, noticiou o New York Times.

Funcionários da NSA continuaram a defender as ações da agência, alegando que os Estados Unidos estariam em risco considerável se mensagens de terroristas e espiões não fossem decifradas.

A informação governamental que trafega pela internet é o poder de proteger e garantir a segurança nacional, mas também de monitorar e atacar outros Estados e após a demonstração do poder governamental dos países do Norte Global sobre a infraestrutura da internet, ficou evidente para o Brasil (e todos os países) que seria necessário investir na criação de tecnologias internas, porque não é possível confiar na integridade da rede.

2.4 Soberania de Dados e Serviços de Computação em Nuvem: O Novo Campo de Batalha Geopolítica

As informações do tópico anterior inspiram uma reflexão sobre o papel da territorialidade da infraestrutura digital na proteção da segurança não só das pessoas, mas do próprio Estado.

Como é estabelecido no art.1º, inciso I da Constituição Federal, a soberania é o fundamento primário da República Federativa do Brasil, posicionando-o acima de qualquer outra disposição, pois para Paupério (1958) a soberania é a qualidade do "Estado que se dirige, rege, governa independentemente por si mesmo" e, de forma complementar, o Jellinek (1973) afirma que "a soberania é uma propriedade, que não é suscetível nem de aumento e nem de diminuição".

Logo em seguida vem o princípio da cidadania, que T.H. Marshal divide em três dimensões: direitos civis, políticos e sociais. Para a análise do papel dos dados pessoais, o foco será nos direitos civis e nas implicações desse novo direito reconhecido no ordenamento jurídico.

O Marco Civil da Internet (Lei nº 12.965/2014) não foi a primeira legislação a tratar do tema de proteção de dados pessoais, mas certamente foi um divisor de águas ao trazer atenção ao tema. A LGPD consolidou o direito na legislação brasileira, mas entrou em vigor de forma parcelada, sendo a primeira parte em 18 de setembro de 2020 e a segunda, em 1º de agosto de 2021.

No período entre a publicação e o início da vigência em 2020, as tensões políticas em torno do tema cresceram e o Conselho Federal da Ordem dos Advogados do Brasil propôs a

Ação Direta de Inconstitucionalidade 6387 contra o inteiro teor da Medida Provisória n. 954/2020. A decisão coube a Ministra Rosa Weber, que deferiu a medida cautelar em 24 de abril de 2020, e reconheceu a proteção aos dados pessoais como um aspecto da personalidade humana:

> Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. (BRASIL, 2020).

Para concluir de forma emblemática e consolidar o direito de forma explícita, este foi incorporado ao artigo 5º, inciso LXXIX da Constituição, por meio da Emenda Constitucional nº 115/2022.

É justo reconhecer o esforço do Governo Federal para tomar atitudes condizentes com a necessidade de preservar a soberania frente ao domínio estadunidense, porque as soluções oferecidas pelas empresas estão integradas em diversos domínios e ofertam conveniência, o que promove o estado de dependência e impõe desafios significativos no que diz respeito à segurança cibernética e à proteção da privacidade.

Não é razoável sugerir o isolamento do Brasil no âmbito das Tecnologias da Informação e da Comunicação (TICs), tampouco seria possível, perante a forte tradição de diplomacia e colaboração internacional, a previsão da operação de transferência internacional de dados na LGPD e a natureza global do espaço digital.

Seguindo essa lógica de conciliação entre os interesses e fomento do desenvolvimento interno, o Governo Federal já vem desenvolvendo iniciativas desde 2018, como a publicação do "Guia Requisitos Mínimos de Privacidade e Segurança da Informação Para Aplicações Web" e o Pregão Eletrônico SRP nº18/2020 – Nuvem "para eventual contratação de empresa especializada para prestação de serviços gerenciados de computação em nuvem, sob o modelo de cloud broker (integrador) de multi-nuvem" pelo Ministério da Gestão e da Inovação em Serviços Públicos; e Estratégia Brasileira para a Transformação Digital (E-Digital) que já está na sua segunda versão, elaborada pelo Ministério da Ciência, Tecnologia e Inovações (MCTI). Nesse documento há uma preocupação de "aprimorar a infraestrutura de redes e bancos de dados da Administração Pública Federal, promovendo a migração do modelo de

armazenamento para dados em nuvem, e ampliando a inteligência e cruzamento de bases de dados".

Mesmo assim, essas iniciativas ainda são insuficientes para retirar o Brasil da posição de mero consumidor de tecnologia para torná-lo autossuficiente (ou até exportador), que seria o cenário desejável sob a perspectiva do "Estado que se governa independentemente por si mesmo".

A gestão e proteção das informações fica prejudicada e suscetível a ataques cibernéticos, espionagem e incidentes de segurança quando os dados ficam nas mãos de atores estrangeiros, principalmente aqueles que construíram sua fortaleza.

3 A INFRAESTRUTURA TANGÍVEL DO TERRITÓRIO DIGITAL

3.1 A Base Léxica da Tecnologia da Informação

Para permitir que o Direito, enquanto ciência interdisciplinar que dialoga com outros campos do saber, possa absorver e compreender as nuances do serviço de computação em nuvem, é importante apresentar as definições dos aspectos relevantes da tecnologia da informação de maneira estruturada e subdividida. Afinal, o debate se centraliza na materialidade da tecnologia da informação para o processamento dos dados.

3.1.1 Dados e banco de dados

O padrão internacional para sistema de gestão da segurança da informação define, na ISO/IEC 2382:2015, que dados são a "representação reinterpretável de informação de maneira formalizada adequada para comunicação, interpretação ou processamento por humanos ou de formas automáticas". Como os dados são a forma de organização, eles podem ser produzidos em circunstâncias analógicas e digitais, mas para fins de delimitação, a circunstância a ser analisada será a digital, na qual os serviços de computação em nuvem se encontram.

O coletivo dos dados inter-relacionados é o banco de dados, a estrutura que, segundo a AWS (2024), é uma coleção sistemática de dados armazenada eletronicamente, que pode incluir diversos tipos de informações, como palavras, números, imagens, vídeos e arquivos. A utilização de um sistema de gerenciamento de banco de dados (DBMS) possibilita o armazenamento, a recuperação e a edição desses dados. Além disso, em sistemas de computador, o termo "banco de dados" pode se referir tanto ao DBMS quanto ao sistema ou aplicativo associado a ele.

Considerando que a maioria dos dados tratados pelos cartórios extrajudiciais são pessoais (comuns e sensíveis), devido à natureza do serviço público, e tutelados pela Lei Geral de Proteção de Dados Pessoais, é necessário ater-se aos princípios descritos no art. 6º da mencionada lei: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Dessa forma, para suportar a necessidade de processamento e armazenamento dos dados, o serviço de computação em nuvem (ou simplesmente “nuvem)” se mostra o mais eficiente.

3.1.2 Computação em nuvem

A origem da computação em nuvem é atribuída a vários indivíduos ao longo do tempo. O cientista da computação John McCarthy é considerado o primeiro a sugerir, entre o final da década de 1950 e início de 1960, o conceito de uso de *timesharing* de computadores, uma técnica que permite a divisão da máquina ao mesmo tempo e aumenta a produtividade do *hardware* para prevenir ociosidade do processador. Acredita-se que no final de 1996 os funcionários da Compaq começaram a utilizar o termo, porém o uso ficou restrito ao ambiente corporativo.

O termo "computação em nuvem" teve seu primeiro uso acadêmico registrado em 1997, quando o Professor Ramnath Chellappa apresentou a palestra *Intermediaries in Cloud-Computing: A New Computing Paradigm* no encontro anual da INFORMS em Dallas. Na ocasião, Chellappa definiu a computação em nuvem como um "paradigma computacional dinâmico, no qual os limites da computação são definidos por uma combinação de exigências tecnológicas, econômicas, organizacionais e de segurança" (CHELLAPPA, 1997; CHELLAPPA; GUPTA, 2002).

Apesar do conceito anterior ser uma referência no meio acadêmico, o National Institute of Standards and Technology – NIST (2011) trouxe a definição técnica utilizada mundialmente:

> O modelo que possibilita acesso ubíquo, conveniente e sob demanda a uma coleção compartilhada de recursos computacionais configuráveis (como redes, servidores, armazenamento) e que podem ser rapidamente provisionados e liberados com mínimo esforço de gestão ou interação com o provedor de serviços.

A definição do NIST nem sempre é papável para todos compreenderem, por isso é razoável trazer uma definição mais acessível, como a que a Microsoft Corporation disponibiliza no site da Azure Cloud:

> É um termo utilizado para descrever uma rede global de servidores, cada um com uma função única. A nuvem não é uma entidade física, mas uma vasta rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Esses servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer conteúdo ou serviços, como transmissão de vídeos, *webmail*, *software* de produtividade para escritórios ou mídias sociais. Em vez de acessar arquivos e dados de um computador local ou pessoal, acesse-os online, de qualquer dispositivo conectado à Internet. As informações estarão disponíveis em qualquer lugar, a qualquer hora.

Com a existência das nuvens é possível manter os bancos de dados disponíveis e suprir a incompatibilidade entre as necessidades modernas de armazenamento e as capacidades dos computadores domésticos ou empresariais. O *hardware*, ou equipamento físico, não consegue

mais atender à demanda de rodar os softwares necessários, como os sistemas operacionais e aplicativos, e armazenar a imensa quantidade de arquivos e dados produzidos.

Através do serviço de nuvem foi possível separar a eficiência do *software* para a produção de arquivos digitais do poder individual da máquina e terceirizar, através de aluguel, a infraestrutura necessária, que consistem em *Data centers*, Servidores e o Serviço de Computação em Nuvem.

Os requisitos para que o serviço seja adequado são apresentadas na tabela abaixo, adaptada de Borges et al. (2011, apud BOTACIM et al., 2016).

1 Características da computação nas nuvens.

Características	**Definição**
Virtualização de recursos	Permite a distinção dos serviços físicos de infraestrutura, facilitando usabilidade por não lidar diretamente com o hardware.
Serviço sob demanda	Consente que o cliente adquira apenas a quantidade de serviço necessária, permitindo maleabilidade ao ser acrescida ou decrescida a qualquer momento.
Independência de localização	Exige que os recursos estejam na internet tornando-se um ponto centralizado de acesso, permitindo que os usuários acessem de onde estiverem.
Elasticidade e estabilidade	Refere-se à condição de disponibilizar ou remover os recursos contratados, tornando-se elástico e escalável com o incremento de recursos.
Medição de serviços	Realiza o cálculo dos serviços utilizados, sendo comparado a serviços de utilidade pública, como água e eletricidade, com pagamento baseado no uso.
Repositório de dados	Os repositórios de dados, responsáveis por alocar informações, são oferecidos dinamicamente a partir da necessidade do cliente.

Fonte: Adaptado de Borges et al. (2011, apud BOTACIM et al., 2016).

Não se pode deixar de destacar que existem alguns tipos de nuvens no mercado. A nuvem construída para atender às demandas de uma única empresa ou organização é classificada como privada; a que é disponibilizada para o grande público consumidor, como o Google Drive, é uma nuvem pública; a nuvem privada que precisou alocar recursos de nuvens públicas devido à necessidade de escalabilidade ou aumento do espaço de armazenamento é

classificada como uma nuvem híbrida; e, por fim, a nuvem comunitária resulta de uma parceria entre entes com necessidades compartilhadas. Nesse formato, é possível construir um ecossistema privado entre algumas partes e, de quebra, atender a requisitos legais de segurança ou conformidade.

A pesquisa TIC Governo Eletrônico de 2023 analisada por Lins (2023) revela que o armazenamento de dados em nuvem é a tecnologia mais adotada pelos órgãos públicos com área de Tecnologia da Informação no Brasil, representando 64% dos casos. A utilização de *e-mails* em nuvem também é significativa. Lins aponta uma predominância de serviços em nuvem no âmbito federal em comparação com o estadual. Ele argumenta que a migração para a nuvem é mais uma resposta adaptativa das empresas prestadoras do que um desenvolvimento autônomo de competências nas esferas governamentais, citando que apenas 27% dos órgãos públicos investiram em capacidades de processamento em nuvem, um elemento vital para impulsionar a transformação digital dos serviços públicos. A pesquisa não contemplou os cartórios extrajudiciais.

Em 2021 o Ministro João Otávio de Noronha do Superior Tribunal de Justiça, no Recurso em Mandado de Segurança nº 66392, decidiu que empresas que prestam serviços de aplicação na internet em território brasileiro estão sujeitas ao ordenamento jurídico nacional, mesmo que seus dados estejam armazenados em nuvem, pois essa estratégia empresarial não interfere na obrigação de observância da legislação brasileira (BRASIL, 2021).

3.1.3 Data center

A estrutura física que possibilita o processamento e armazenamento em larga escala dos dados digitais é o *data center*. De acordo com Cilento Filho (2024), um *data center* é uma infraestrutura dedicada à centralização, interconexão e operação de equipamentos de tecnologia da informação e redes de telecomunicações, responsável por fornecer serviços de armazenamento, processamento e transporte de dados.

Esses projetos precisam atender vários requisitos ambientais, conforme explicado pela Amazon Web Services (AWS) em sua página do site oficial: Subsistemas de energia; Fontes de alimentação ininterruptas (UPS); Geradores reservas; Equipamentos de ventilação e arrefecimento; Sistemas de combate a incêndios; Sistemas de segurança de edifícios.

Adicionalmente, as instalações precisam ser redundantes e geograficamente espalhadas para poder assegurar a resistência da rede em caso de comprometimento (como ataques, desastres ambientais etc.) de um prédio e assegurar que todo o tráfego da rede possa ser

redirecionado para outra localização que provavelmente estará segura e impedirá a perda de um Servidor.

A estrutura que permite esse nível de estabilidade e eficiência é complexa, custosa e de difícil desenvolvimento. De acordo com a Fundação Seade, a construção de um *data center* foi avaliada em R$ 15,6 bilhões (quinze bilhões e seiscentos milhões de reais) pela empresa estadunidense CloudHQ. O empreendimento será construído em Paulínia - SP e teve um impacto significativo nos investimentos do estado de São Paulo, representando cerca de um terço dos R$ 45,7 bilhões (quarenta e cinco bilhões e setecentos milhões de reais) anunciados nos municípios paulistas entre janeiro e junho de 2024.

O projeto da CloudHQ contempla a oferta de até 288 MW (megawatts de potência elétrica) de capacidade de carga de TI, distribuída em seis edifícios, com um investimento total estimado em US$ 3 bilhões (três bilhões de dólares americanos), divididos em duas fases. A primeira fase inclui três edifícios com 48 MW cada, enquanto a segunda fase segue a mesma configuração.

A pesquisa “Global Cloud Ecosystem Index 2022” conduzida pelo MIT Technology Review faz uma avaliação e classificação dos serviços de computação em nuvem de 76 países, o Brasil se encontrava na posição 52 com a classificação “este pilar mede a maturidade dos ambientes regulatórios que promovem ambientes de segurança e soberania de dados progressivos e voltados para a nuvem, além de permitir a confiança em recursos digitais.” (MIT Technology Review; Infosys, 2022).

A maioria das empresas privadas estadunidenses construíram seus *data centers* por todo o mundo, como a Microsoft Azure (2024) que disponibiliza no seu site um mapa dos países em cada continente, como Estados Unidos, Canadá, Brasil, México, Chile nas Américas; Alemanha, França, Reino Unido, Países Baixos, Noruega, Suécia na Europa; Austrália, Japão, Índia, Coreia do Sul, Cingapura na Ásia-Pacífico e Emirados Árabes Unidos, Catar, África do Sul no Oriente Médio e África. Existe um motivo muito prático para a presença global: quando os servidores e bancos de dados estão próximos dos usuários é possível reduzir a distância física que os dados precisam percorrer e minimizar o roteamento ineficiente e os saltos na rede.

A sobrevivência das infraestruturas pode ser aumentada ao distribuir *data centers* em diferentes locais de uma região geográfica, minimizando riscos relacionados a falhas interconectadas, como rompimentos de fibras ópticas ou quedas de energia. Contudo, apesar dos efeitos positivos da distribuição geográfica de centros de dados, o projeto deve considerar o aumento da latência (medida de atraso) na comunicação entre servidores devido à maior distância entre eles e o acréscimo dos custos de interconexão (Couto et al., 2014).

O Servidor consegue rodar no seu sistema operacional especializado todas as operações solicitadas por outros computadores, gerenciar os recursos da rede, armazenar, enviar e processar dados porque os *data centers* provêm o *hardware* necessário, grande disponibilidade de rede de internet e funcionam ininterruptamente. Existem diversos tipos de Servidores, cada um designado para atender a necessidades particulares, como armazenamento e distribuição de arquivos, gerenciamento de e-mails, hospedagem de sites e suporte a grandes bases de dados.

Os Servidores possuem núcleos de processador e grande capacidade de armazenamento, permitindo o fornecimento de serviços computacionais robustos por meio de grupos interconectados. Já as redes conectam diferentes recursos da nuvem, como aplicações e armazenamentos, utilizando equipamentos como balanceadores de carga para gerenciar o tráfego e melhorar a performance dos sistemas, especialmente em momentos de alta demanda.

Portanto, no ciclo da infraestrutura da tecnologia da informação, a ponta final da operação é o serviço de computação em nuvem que vai centralizar todas as operações para entregar os dados, aplicações e serviços aos usuários finais.

O relatório "Estratégia Brasileira para a Transformação Digital (E-Digital) - Ciclo 2022-2026" (BRASIL, 2022) fez uma análise detalhada sobre a presença de *data centers* no território nacional e constatou que a ausência destes, mesmo entre as capitais, é uma grande desvantagem. O Brasil tem dimensões continentais, vastas fronteiras terrestres com outros países latino-americanos e o grande mercado doméstico, especialmente quando comparado com a ampla disseminação desses centros nos Estados Unidos e na Europa. O Brasil detém, na América Latina, a maior quantidade de cabos submarinos e o maior número de *data centers*, com 74 unidades distribuídas em 20 municípios.

Por fim, o relatório sugere a elaboração de políticas e incentivos públicos para aquecer o mercado e trazer investimentos para o país.

A Agência Brasileira de Desenvolvimento Industrial (ABDI) em parceria com o Ministério do Desenvolvimento, Indústria, Comércio e Serviços lançou em 2023 o estudo "Estratégia para a implementação de política pública para atração de Data Centers". A iniciativa busca abarcar todos os requisitos necessários para o êxito da tarefa e para isso, segue as seguintes etapas:

> 1. Mapeamento das oportunidades de instalação de data centers para prestação de serviços a terceiros no país, com base na análise da demanda regional e da oferta dos provedores de serviços de data centers.
> 2. Levantamento dos custos de construção e operação de um data center no Brasil seguindo padrões internacionais, comparando com países vizinhos da América do Sul.

> 3. Mapeamento das políticas públicas adotadas por outros países para o segmento de data centers, incluindo a análise do ambiente regulatório dos países analisados.
> 4. Análise comparativa de competitividade entre o Brasil e os países vizinhos para realização de investimentos em data centers.
> 5. Identificar fatores críticos de sucesso para o desenvolvimento de serviços de data center no país, com foco em marcos regulatórios e ambiente de negócios para estimular o mercado.
> 6. Proposição de uma estratégia de política pública para atração de provedores de data center.

3.1.4 Backup

A ISO/IEC 2382:2015 estabelece que o *backup* pode ser um procedimento, técnica ou hardware utilizado para auxiliar na recuperação de dados perdidos ou destruídos ou para manter um sistema em funcionamento. Essa criação de cópias de segurança dá continuidade às operações, permitindo a rápida restauração de pontos críticos com impacto mínimo para que os sistemas não fiquem inoperantes por períodos prolongados ou até mesmo se tornem irrecuperáveis, mesmo com o auxílio de especialistas (AWS, 2024).

É a partir desse *framework,* para proteger o acervo visando a "segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil", que o Provimento nº 74/2018 do Conselho Nacional de Justiça pôde requisitar o backup em todas as suas possibilidades. Através do procedimento/técnica de *backup* o arquivamento dos livros e atos eletrônicos em deve ser "feito em intervalos não superiores a 24 horas" com a possibilidade de recuperação de pelo menos "30 minutos antes da ocorrência de evento que comprometa a base de dados e informações associadas". Para garantir a multiplicidade de cópias, é obrigatória a realização em mídia eletrônica (a ser armazenada em local distinto da instalação da serventia) e cópia de segurança na internet.

Concomitantemente "a plataforma de banco de dados deverá possuir recurso de trilha de auditoria ativada" para garantir o rastreamento das falhas, essas informações também precisam ser preservadas em *backup*, bem como a criação de uma política de segurança da informação que deve "ter um plano de continuidade de negócios que preveja ocorrências nocivas ao regular funcionamento dos serviços" e "atender a normas de interoperabilidade, legibilidade e recuperação a longo prazo na prática dos atos e comunicações eletrônicas".

O Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco também define:

> Art. 94. Para fins da aplicação deste Código de Normas e demais disposições legais e regulamentares, quando aos atos eletrônicos ou digitais, considera-se:

> VIII – cópia de segurança: estrutura de arquivamento redundante (*backup*) dos bancos de dados armazenados na serventia, de modo a garantir a segurança, a integridade e a inviolabilidade de seu conteúdo, que deve ser feita diariamente, em intervalos não superiores a 24 horas;

Todos os atos registrais e notariais estão em sistema que geram relatórios para os órgãos públicos, ou a alimentação (como a Central Eletrônica Notarial de Serviços Compartilhados - CENSEC ou a Declaração sobre Operações Imobiliárias (DOI) à Receita Federal) das plataformas ou de fiscalização em âmbito nacional, a fim de garantir, através da autenticação, a troca de informações.

O Provimento Nº 149 de 30/08/2023 (Institui o Código Nacional de Normas da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça - Foro Extrajudicial (CNN/ CN/CNJ-Extra), que regulamenta os serviços notariais e de registro) traz no seu art. 93 que "o responsável pela serventia extrajudicial, sempre que possível: I - digitalizará os documentos físicos ainda utilizados; e II - armazenará os documentos físicos que contenham dados pessoais e dados pessoais sensíveis em salas ou compartimentos com controle de acesso", de forma que frisa o esforço para alimentar o ecossistema digital nacional e assegure a qualidade do banco de dados.

Considerando que a atividade cartorária é uma delegação do Poder Público, a escolha dos serviços a serem utilizados cabe ao registrador ou tabelião, que detém a prerrogativa de selecionar o serviço mais adequado às necessidades do cartório. Tais decisões, invariavelmente, estão relacionadas às condições financeiras do cartório, conforme o Provimento nº 74 que classifica: CLASSE 1 – Serventias com arrecadação de até R$ 100 mil (cem mil reais) por semestre, correspondente a 30,1% dos cartórios extrajudiciais; CLASSE 2 – Serventias com arrecadação entre R$ 100 mil (cem mil reais) e R$ 500 mil (quinhentos mil reais) por semestre, correspondente a 26,5% dos cartórios extrajudiciais; CLASSE 3 – Serventias com arrecadação superior a R$ 500 mil (quinhentos mil reais) por semestre, correspondente a 21,5% dos cartórios extrajudiciais.

A classificação reconhece e adequa os requisitos não só pelo volume de dados produzidos, mas, principalmente, pelo orçamento disponível. Essa variável deve ser sempre considerada, já que a materialidade das possibilidades depende dos recursos financeiros.

Na pesquisa quantitativa, que será abordada em detalhes no próximo capítulo, foi possível identificar que a nuvem Microsoft 365/Onedrive é o serviço mais utilizado pelos respondentes do formulário.

Dessa forma, é relevante realizar uma investigação sobre a percepção de segurança, considerando que a Microsoft é uma das empresas mais utilizadas no mundo e com boa aceitação pelo público brasileiro, a fim de verificar casos significativos de incidentes de segurança. A análise deve, ainda, estabelecer uma conexão com o fato que a empresa também fornece o ecossistema de *software* do Poder Público dos Estados Unidos, um país com práticas comprovadas de espionagem governamental.

3.2 A concentração do poder tecnológico da Microsoft Corporation: pesquisa documental sobre incidentes de segurança cibernética da empresa.

Com quase 50 anos, a Microsoft Corporation é uma das empresas mais antigas e consolidadas no mercado de tecnologia da informação, por isso, possui o benefício da familiaridade e uso difundido.

A percepção de confiança vem sendo questionada no meio da tecnologia diante dos vários incidentes de segurança. De janeiro de 2020 até agosto de 2024 foram reportadas 4.677 vulnerabilidades nos produtos da Microsoft Corporation para a base pública de dados Common Vulnerabilities and Exposures (CVE, 2024). Torna-se imperativo questionar se, para além da confiança habitual nas *big techs*, essa empresa é realmente segura para o uso institucional do Poder Público brasileiro.

Os dois casos foram selecionados com base no critério de maior volume de dados comprometidos ou maior vulnerabilidade, especialmente nos casos de invasão por *hackers*.

Para investigar a integridade e a segurança dos modelos de computação em nuvem oferecidos pela Microsoft, foi adotada uma metodologia heterogênea de estudo de artigos de jornais que cobriram os incidentes, publicações especializadas em segurança da informação, bancos de dados de vulnerabilidades conhecidas, relatórios de incidentes divulgados tanto pela Microsoft quanto por agências de segurança cibernética, bem como análises independentes encontradas em blogs e fóruns especializados. Além disso, a consulta de normas padrão para sistemas de gestão da segurança da informação.

A análise foi conduzida em ordem cronológica, que permite uma experiência fluida do progresso e das lacunas na abordagem de segurança da empresa, crucial para este estudo.

2 Resumo da Metodologia – Pesquisa Documental

Propósito	Analisar, à luz dos casos mais recentes, se a Microsoft Corporation, identificada na pesquisa quantitativa como a mais utilizada, é de fato a mais segura, considerando a percepção de segurança e qualidade a ela atribuída.
Forma de coleta dos dados	Levantamento e análise dos casos registrados: Na base de dados Common Vulnerabilities and Exposures de janeiro de 2020 até agosto de 2024; Reportagens de jornais; Pronunciamentos oficiais da empresa Microsoft; Documentos emitidos por congressistas estadunidenses; e Dossiês publicados em blogs oficiais por especialistas da área de segurança da informação.
Casos Escolhidos	Julho de 2023: Invasão da plataforma de e-mail da Microsoft e roubo de e-mails do Departamento de Estado dos EUA; Janeiro de 2024: Hackers russos utilizaram a técnica de "Pulverização de Senhas" para invadir a Microsoft em novembro de 2023.
Critério de escolha dos Casos	Maior volume de dados comprometidos ou maior exposição a vulnerabilidades, especialmente em casos de invasões por hackers e os danos decorrentes.

Fonte: Elaborado pela autora (2024).

3.2.1 Casos de Incidentes de Segurança

Em 2024 a Autoridade Nacional de Proteção de Dados Pessoais conceituou um incidente de segurança, em consonância com a norma internacional ISO/IEC, como "qualquer evento adverso que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade da segurança do sistema dados pessoais".

Os provedores de serviço de computação em nuvem constantemente fazem testes de penetração e emulam ataques para fortalecer a segurança, porém, quando uma vulnerabilidade é explorada os danos são extensos e imprevisíveis.

3.2.1.1 Julho de 2023: Invasão da plataforma de e-mail da Microsoft e roubo de e-mails do Departamento de Estado dos EUA.

De acordo com a Microsoft, um grupo de hackers identificado como Storm-0558 ligados ao governo chinês utilizou tokens de autenticação digital falsificados, através do comprometimento da conta um engenheiro com um "malware de roubo de token", para invadir contas de e-mails operadas através dos serviços Outlook.com e Exchange Online.

A invasão resultou no roubo de aproximadamente 60.000 e-mails de 10 contas do Departamento de Estado e de altos funcionários americanos, incluindo a Secretária de Comércio Gina Raimondo, o Embaixador dos EUA na China Nicholas Burns e o Secretário Assistente de Estado para a Ásia Oriental, Daniel Kritenbrink.

Essa situação trouxe reflexões sobre o papel predominante da Microsoft na prestação de serviços de Tecnologia da Informação para o governo dos EUA. O porta-voz dos Estados Unidos não comentou sobre a atribuição de culpa e o governo da China negou o ataque.

Shir Tamari, o chefe de pesquisa da empresa Wiz.io, publicou no blog da empresa uma matéria informando que o ataque foi mais impactante do que a avaliação inicial com o relatório da investigação feita e recomendações para as organizações que utilizam a Microsoft e Azure.

O principal resultado da investigação foi a descoberta que a chave de assinatura que foi comprometida não estava limitada somente aos dois serviços de e-mail e era poderosa o suficiente para forjar tokens de acesso para vários tipos de aplicações que tem a funcionalidade "login com Microsoft" dos serviços do Azure Active Directory, incluindo todas as aplicações como SharePoint, Teams e OneDrive. O grupo Storm-0558 conseguiu acesso a várias chaves de acesso e autenticação (Tamari, 2023).

Em maio de 2024 os senadores Eric S. Schmitt e Ron Wyden enviaram uma carta ao Departamento de Defesa dos Estados Unidos questionando a decisão preliminar do Pentágono de fazer o upgrade do serviço de computação em nuvem da Microsoft 365 para o Office 365 E5.

Na carta eles expressam preocupação em relação a abordagem, pois a cibersegurança deveria ser considerada uma característica essencial do software, e não um recurso premium vendido a preços elevados para clientes governamentais e corporativos com grandes recursos financeiros.

Por fim, lembram que a dependência do governo dos Estados Unidos em relação à Microsoft mostrou-se problemática quando o Storm-0558, conseguiu invadir 22 organizações empresariais e mais de 500 indivíduos ao redor do mundo, explorando vulnerabilidades nos

sistemas de e-mail de importantes departamentos governamentais como o Departamento de Estado, o Departamento de Comércio e a Câmara dos Representantes dos EUA.

O Conselho de Revisão de Segurança Cibernética (CSRB) caracterizou esse incidente como resultado de "uma cascata de falhas" por parte da Microsoft, que facilitou o acesso dos hackers a milhares de e-mails sensíveis de altos funcionários, incluindo correspondências de membros do alto escalão do Departamento de Estado e do Secretário de Comércio (Schmitt & Wyden, 2024).

3.2.1.2 Janeiro de 2024: Hackers russos utilizaram a técnica de "Pulverização de Senhas" para invadir a Microsoft em novembro de 2023

A Microsoft publicou no seu blog "Microsoft Security Response Center (MSRC)" o anúncio do ataque realizando pelo grupo russo chamado Midnight Blizzard ou NOBELIUM, que os Estados Unidos e o Reino Unido atribuem ao Serviço de Inteligência Estrangeira da Federação Russa, que aconteceu continuadamente durante os meses de novembro de 2023 e janeiro de 2024.

A ofensiva aconteceu através da técnica de pulverização de senha e comprometeu o sistema de e-mail corporativo de membros de equipe de liderança sênior e funcionários das áreas de cibersegurança, jurídica, entre outras, exfiltrando alguns e-mails e documentos anexos, bem como tentou acessar repositórios de código-fonte e outros sistemas internos.

Steve Bellovin, pesquisador em redes e segurança de computadores e professor do departamento de ciência da computação da Universidade de Columbia, publicou na rede social "Mastodon" suas considerações sobre as sérias implicações desse ataque, conjecturando que provavelmente as contas de liderança continuavam usando apenas as permissões de uma "conta de teste de administrador", sem a autenticação de dois fatores ativada e com senhas muito fracas (Bellovin, 2024).

Após a extensa revisão da bibliografia, a escolha do recorte revelou-se particularmente adequada. Na rotina automática do dia a dia os casos aqui compilados se perdem entre uma notícia e outra e são apagados através de constantes campanhas de marketing.

Apesar de a Microsoft ser uma empresa tradicional no ecossistema da internet, nos últimos quatro anos, a empresa enfrentou uma crise contínua de incidentes de segurança, marcada por graves problemas de segurança e integridade dos seus sistemas e de clientes.

Além disso, a natureza dos ataques atribuídos a hackers chineses e russos permite concluir que o serviço de computação em nuvem não apenas representa um campo de disputa, mas também é efetivamente um palco para conflitos geopolíticos.

3.3 Análise de pesquisas de mercado sobre confiabilidade nos serviços de computação em nuvem

O Brasil se destaca como um dos países mais afetados por ciberataques, como demonstra o relatório *Trend Micro 2023 Midyear Cybersecurity Threat Report* da empresa de antivírus Trend Micro, "os Estados Unidos, Brasil e Índia tiveram os eventos de risco mais detectados no primeiro semestre de 2023" e, segundo o estudo *Cost of a Data Breach Report 2023* do IBM Security, enfrentamos em 2023 prejuízos significativos que alcançaram a cifra de US$1.22 milhões (um milhão e duzentos e vinte mil dólares americanos) em incidentes de segurança na iniciativa privada.

As empresas e o setor público têm demonstrado uma tendência crescente em optar por fornecedores globais de computação em nuvem, percebidos como mais seguros e confiáveis em comparação aos serviços locais. Essa preferência por provedores internacionais é influenciada pela superioridade técnica percebida, conformidade com padrões internacionais de segurança da informação e valores do serviço. Assim, a confiança nas soluções globais reflete uma busca por maior proteção contra as ameaças cibernéticas que continuam a desafiar o Brasil. O estudo *Data Privacy Benchmark Study 2023* da Cisco Systems, Inc. elabora o panorama:

> Muitos governos e organizações estão estabelecendo requisitos de localização de dados, que forçam a manutenção de dados dentro de um país ou região. Para muitos, estes requisitos parecem uma boa ideia no início, mas nossa pesquisa indica que esta visão não se sustenta uma vez considerados os custos, a segurança, a privacidade e outras compensações. Na Pesquisa de Privacidade do Consumidor Cisco 2022, por exemplo, 78% dos consumidores disseram inicialmente que achavam que a localização de dados era uma boa ideia, mas o suporte caiu para 41% ao incluir o custo adicional de bens e serviços. De acordo com 89% dos consumidores das organizações na pesquisa deste ano, a localização de dados acrescenta um custo significativo às suas operações.
>
> Os resultados deste estudo atual mostram que a grande maioria (88%) dos entrevistados acredita que seus dados seriam intrinsecamente mais seguros se fossem armazenados apenas dentro de seu país ou região. Notavelmente, um número ainda maior (90%) também disse que um fornecedor global, operando em escala, pode proteger melhor os dados em comparação com fornecedores locais. Ao ver estas duas afirmações juntas, parece que, embora as organizações preferissem manter seus dados locais, elas ainda preferem e confiam em um fornecedor global em vez de um fornecedor local.

Mesmo que os entrevistados na pesquisa da CISCO admitam que o cenário ideal para a proteção dos dados da organização seria no território nacional, a localização dos servidores influencia no custo operacional do serviço, fator que costuma se sobrepor nas decisões tomadas e pode tornar a concorrência desleal.

A influência exercida pelos oligopólios tecnológicos estadunidenses pode ser interpretada como uma reinvenção e evolução do processo compulsório de acumulação de riqueza. Nesse sentido, a hegemonia dessas corporações não apenas reproduz as dinâmicas clássicas de acumulação de capital, mas também inaugura novas formas de controle e dependência, promovendo uma centralização de recursos e informações sem precedentes na história recente.

4 O USO DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM NOS CARTÓRIOS EXTRAJUDICIAIS DE PERNAMBUCO: PESQUISA E PROJETO DE GOVERNANÇA

4.1 A formalidade documental da pessoa natural: A importância da segurança jurídica proporcionada pelos serviços cartorários extrajudiciais

Após uma análise cruzada entre a Constituição Federal, o Código Civil, a Lei nº 8.935/94 (Lei dos Cartórios extrajudiciais) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) é possível afirmar que os cartórios extrajudiciais formam a base de dados pessoais do povo brasileiro, que, por sua vez, sustenta toda a estrutura do Estado brasileiro

Dentre as muitas atribuições dos cartórios extrajudiciais, o recorte que melhor ilustra a conjuntura, e escolhido com base no maior grupo respondente da pesquisa quantitativa, é a atribuição da lavratura do Registro Civil no livro "A" e a emissão do primeiro documento com validade jurídica da pessoa natural: a Certidão de Nascimento – a partir desse ponto o cidadão brasileiro existirá oficialmente para o Estado. É o ato de assento do nascimento de uma pessoa feito no livro próprio de registro civil de nascimento (nascidos vivos). "O registro de nascimento dá publicidade ao nascimento com vida de determinada pessoa, conferindo-lhe existência legal e autêntica, atribuindo-lhe aptidão para contrair obrigações e adquirir direitos" (TJDFT, 2019).

Todas as grandes etapas da vida de quem foi registrado são documentadas no cartório, conforme o art. 29 da Lei n. 6.015/1973: o nascimento, a alteração/retificação do nome e a adequação de gênero; o casamento civil e os proclamas; a conversão de união estável em casamento; o casamento religioso; o óbito; a emancipação; a interdição; a sentença declaratória de ausência; a sentença que defere a legitimação adotiva; a perda e a suspensão do poder familiar; o reconhecimento ou exclusão da filiação; a perda e a reaquisição da nacionalidade brasileira.

Pela leitura da Lei de Registros Públicos é possível observar que o Estado tenta esgotar as possibilidades da responsabilidade do registro da criança:

> Art. 52. São obrigados a fazer declaração de nascimento:
> 1. O pai ou a mãe, isoladamente ou em conjunto, observado o disposto no § 2o do art. 54;
> 2. No caso de falta ou de impedimento de um dos indicados no item 1o, outro indicado, que terá o prazo para declaração prorrogado por 45 (quarenta e cinco) dias;
> 3. No impedimento de ambos, o parente mais próximo, sendo maior achando-se presente;

4. Em falta ou impedimento do parente referido no número anterior os administradores de hospitais ou os médicos e parteiras, que tiverem assistido o parto;
5. Pessoa idônea da casa em que ocorrer, sendo fora da residência da mãe;
6. Finalmente, as pessoas encarregadas da guarda do menor.

O reconhecimento formal não é responsabilidade exclusiva dos pais, mas de toda a comunidade em que a pessoa nasceu, que precisam estar munidas da Declaração de Nascido Vivo (DNV) ou dos requisitos listados no art. 37, a exemplo de: o nome do registrado; o número da matrícula; o dia, o mês, o ano, o município e a unidade da federação do nascimento; o município e a unidade da federação do registro; o sexo do registrado; o nome e a naturalidade dos pais; o nome dos avós; quando o caso de o registrado ser gêmeo, o nome do irmão e o número da matrícula.

O texto de justificativa do Provimento Nº 151 de 26/09/2023, que dispõe sobre o registro do natimorto e estabelece o procedimento de promoção do registro de nascimento de criança ou adolescente no caso de omissão, da Corregedoria Nacional de Justiça trouxe as legislações pertinentes ao tema:

1. Código Civil (Lei nº 10.406/2002) - Art. 16: "Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome."
2. Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) - Art. 102: Prevê a regularização do Registro Civil.
3. Pacto Internacional sobre Direitos Civis e Políticos (Decreto nº 592/1992) - Art. 24, item 2: "Toda criança deverá ser registrada imediatamente após seu nascimento e deverá receber um nome."
4. Convenção Internacional sobre os Direitos da Criança (Decreto nº 99.710/1990) - Arts. 7, item 1, e 8, item 2: Estabelece o direito da criança ao registro, nome, nacionalidade e à assistência para restabelecimento da identidade, se necessário.
5. Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica) (Decreto nº 678/1992) - Art. 18: "Toda pessoa tem direito a um prenome e aos nomes de seus pais ou de um destes. A lei deve regular a forma de assegurar a todos esses direitos, mediante nomes fictícios, se for necessário."

A partir desse rico arcabouço, os cartórios extrajudiciais, segundo a Lei nº 8.935/94 têm a obrigação de “comunicar o registro ao Ministério da Economia e ao INSS pelo Sistema Nacional de Informações de Registro Civil (Sirc) ou por outro meio que venha a substituí-lo” e em geral, de alimentar as outras bases de dados do Estado.

Essa comunicação a outros órgãos permite que o Instituto Brasileiro de Geografia e Estatística (IBGE) possa fazer o cruzamento das Estatísticas do Registro Civil com bases de dados do Ministério da Saúde, como o Sistema de Informações sobre Nascidos Vivos (SINASC) e o Sistema de Informações sobre Mortalidade (SIM) para trazer as importantes estatísticas presentes no "Estudo Complementar à Aplicação da Técnica de Captura-Recaptura", que apresentou as estimativas de sub-registro e subnotificação de nascimentos e óbitos no Brasil para o ano de 2022.

Foram estimados 2.574.556 nascidos vivos e o percentual de sub-registro foi de 1,31% (33.726 nascimentos), o menor da série histórica iniciada em 2015; e 1.561.339 óbitos no país. A proporção de sub-registro foi 3,65% (56.988 óbitos), percentual superior ao do ano anterior (3,49%). (IBGE, 2022).

O estatístico do IBGE, José Eduardo Trindade, destacou que essa redução de sub-registro de nascidos vivos é fruto de ações legislativas, como "o marco legal da primeira infância, foi determinado que o Registro Civil fosse realizado nas unidades interligadas da maternidade, permitindo que a criança já saísse com o registro feito". A curva de melhora se mostra promissora, porém ainda temos, em números estimados, 33.726 pessoas fora do radar do Estado. (IBGE, 2022).

Esses dados embasam a criação de políticas públicas e inciativas que procuram integrar as pessoas a cidadania. A invisibilidade prejudica e pode até impedir a materialização dos direitos constitucionais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância. É possível adicionar a impossibilidade de acessar linhas de crédito, suporte da assistência social e habilitação para iniciativas de políticas de afirmação e inclusão, emissão da Carteira Nacional de Habilitação, Título de Eleitor ou a Carteira de Trabalho e a garantia formal de propriedade de bens.

A busca pelo reconhecimento da pessoa humana também se estende para a identificação dos óbitos e desaparecimentos. Em 2015 foi criada a base de dados "Óbitos desconhecidos" para atender a Recomendação nº 19 do Conselho Nacional de Justiça (CNJ), editada pela ministra Nancy Andrighi, a ARPEN disponibiliza a "Central Nacional de Óbitos de Pessoas Não Identificadas", que auxilia a busca de informações relacionadas a desaparecidos dentro da base de dados da CRC Nacional. Os dados publicados até novembro/2024 mostram a dificuldade de encontrar essas pessoas:

1. Óbitos cadastrados - 53.894.158
2. Óbitos desconhecidos - 665.181

3. Óbitos reconhecidos - 6.518

A porcentagem de óbitos desconhecidos é aproximadamente 1,23%, enquanto a de óbitos reconhecidos é cerca de 0,01% em relação ao total cadastrado.

A iniciativa também busca preencher as lacunas na história e encontrar respostas para esclarecer e não esquecer.

4.1.1 A qualidade do banco de dados

A Lei dos Cartórios, em seu artigo 3º, estabelece expressamente que "o notário, ou tabelião, e oficial de registro, ou registrador, são profissionais do direito, dotados de fé pública, a quem é delegado o exercício da atividade notarial e de registro". Isso significa que os documentos por eles emitidos são considerados válidos e possuem força de "prova plena", conforme o artigo 215 do Código Civil.

Essa disposição cria a presunção de um banco de dados que cumpre, na medida do possível, o princípio de "precisão" disposto na ISO/IEC 2382:2015: qualidade do que está livre de erros. Como a atualização depende da vontade ou possibilidades (econômicas, de saúde e deslocamento, grau de escolaridade etc.) das pessoas, na realidade a qualidade pode ser prejudicada.

Em uma Certidão de Nascimento são tratados dados pessoais de crianças e adolescentes, uma categoria de titulares que tem uma proteção extra da LGPD, dados sensíveis, que também exigem medidas robustas.

Como o serviço de Cartório Extrajudicial é uma delegação do Poder Público, a LGPD fez a equiparação expressa no § 4º do art. 23 às pessoas jurídicas de direito público. No guia orientativo "Tratamento de dados pessoais pelo Poder Público" (ANPD, 2023) o conceito de obrigação legal, presente nos artigos 7º, II, e 11, II, "a", é reforçado pelo disposto no artigo 23, que determina que o tratamento de dados pessoais no setor público deve visar a execução de competências legais ou o cumprimento de atribuições do serviço público, sempre com observância do interesse público e da finalidade específica.

A cultura de proteção de dados pessoais ainda é imatura no Brasil, visto que a Lei só entrou completamente em vigor em agosto de 2021. É pertinente salientar que, das oito decisões em processos sancionadores publicadas no site da ANPD até agosto de 2024, apenas um envolveu um agente de tratamento era uma empresa privada:

1. Relatório de Instrução nº 4/2023/FIS/CGF/ANPD - Secretaria de Estado da Saúde de Santa Catarina.

2. Relatório de Instrução n° 3/2023/CGF/ANPD - Instituto de Pesquisas Jardim Botânico do Rio de Janeiro - JBRJ.
3. Relatório de Instrução n° 2/2023/CGF/ANPD - Instituto de Assistência ao Servidor Público Estadual de São Paulo - IAMSPE.
4. Relatório de Instrução n° 1/2023/CGF/ANPD - Telekall Inforservice.
5. Relatório de Instrução nº 1/2024/CGF/ANPD - Instituto Nacional do Seguro Social - INSS.
6. Relatório de Instrução nº 2/2024/FIS/CGF/ANPD - Secretaria de Estado de Educação do Distrito Federal (SEEDF).
7. Relatório de Instrução nº 3/2024/FIS/CGF/ANPD - Secretaria de Assistência Social, Combate à Fome e Políticas sobre Drogas (SAS), sucessora da Secretaria de Desenvolvimento Social, Criança, Juventude e Prevenção à Violência e às Drogas do Estado de Pernambuco (SDSCJPVD), que sucedeu a Secretaria de Desenvolvimento Social, Criança e Juventude de Pernambuco (SDSCJ).
8. Relatório de Instrução nº 4/2024/FIS/CGF/ANPD - Ministério da Saúde.

Não é possível afirmar que o Estado é o maior violador do direito do titular, visto que a ANPD ainda não está completamente equipada para processar todas as denúncias que são feitas pelo canal oficial, mas diante da análise dos casos acima listados é compreensível o receio em relação a forma que o Estado brasileiro trata os dados pessoais dos seus cidadãos.

4.2 O Provimento nº 74 de 31/07/2018

O ato normativo que motivou toda a pesquisa é o Provimento nº74 que "dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil e dá outras providências", editado e publicado pelo Conselho Nacional de Justiça.

A motivação traz três pontos importantes para uma visão holística:

1. O avanço tecnológico impulsionou a informatização e a adoção de sistemas eletrônicos compartilhados, permitindo a realização de atividades notariais e de registro com suporte em tecnologias da informação e comunicação;
2. A uniformização na manutenção de arquivos eletrônicos e mídias digitais de segurança se mostra essencial para garantir a integridade, a eficiência e a confiabilidade dos documentos e registros;

3. As inspeções anteriores evidenciaram vulnerabilidades e riscos na gestão das bases de dados, reforçando a necessidade de medidas que fortaleçam a segurança e a continuidade dos serviços notariais e de registro.

Para que a leitura da pesquisa seja fluida, os artigos que serão alvo do estudo estão listados a seguir:

> Art. 3º Todos os livros e atos eletrônicos praticados pelos serviços notariais e de registro deverão ser arquivados de forma a garantir a segurança e a integridade de seu conteúdo.
> § 1º Os livros e atos eletrônicos que integram o acervo dos serviços notariais e de registro deverão ser arquivados mediante cópia de segurança (backup) feita em intervalos não superiores a 24 horas.
> § 2º Ao longo das 24 horas mencionadas no parágrafo anterior, deverão ser geradas imagens ou cópias incrementais dos dados que permitam a recuperação dos atos praticados a partir das últimas cópias de segurança até pelo menos 30 minutos antes da ocorrência de evento que comprometa a base de dados e informações associadas.
> § 3º A cópia de segurança mencionada no § 1º deverá ser feita tanto em mídia eletrônica de segurança quanto em serviço de cópia de segurança na internet (backup em nuvem).
> § 4º A mídia eletrônica de segurança deverá ser armazenada em local distinto da instalação da serventia, observada a segurança física e lógica necessária.
> § 5º Os meios de armazenamento utilizados para todos os dados e componentes de informação relativos aos livros e atos eletrônicos deverão contar com recursos de tolerância a falhas.

> Art. 5º O sistema informatizado dos serviços notariais e de registro deverá ter trilha de auditoria própria que permita a identificação do responsável pela confecção ou por eventual modificação dos atos, bem como da data e hora de efetivação.
> § 1º A plataforma de banco de dados deverá possuir recurso de trilha de auditoria ativada.
> § 2º As trilhas de auditoria do sistema e do banco de dados deverão ser preservadas em backup, visando a eventuais auditorias.

> Art. 7º Os serviços notariais e de registro deverão adotar rotina que possibilite a transmissão de todo o acervo eletrônico pertencente à serventia, inclusive banco de dados, softwares e atualizações que permitam o pleno uso, além de senhas e dados necessários ao acesso a tais programas, garantindo a continuidade da prestação do serviço de forma adequada e eficiente, sem interrupção, em caso de eventual sucessão.

As diretrizes se mostram condizentes com os padrões internacionais de segurança, bem como a lógica de prevenção de incidentes de segurança e redução de danos. O banco de dados do *backup* deve ser atualizado quase que em tempo real, com a responsabilidade de permitir trilha de auditoria e a portabilidade completa do acervo, independente do sistema utilizado.

4.3 Uso de Computação em Nuvem nos Cartórios extrajudiciais de Pernambuco: pesquisa quantitativa por amostragem.

4.3.1 Metodologia

Considerando que, mesmo em um cenário ideal, seria inviável avaliar a realidade dos mais de 15 mil cartórios extrajudiciais de registro e tabelionatos de notas e protestos existentes no Brasil, optou-se por delimitar o estudo ao estado de Pernambuco e focar apenas na contabilização da escolha do serviço de computação em nuvem contratado.

Todos os dados a serem analisados nesse capítulo foram coletados através do questionário intitulado "Pesquisa Acadêmica sobre o Uso de Computação em Nuvem nos Cartórios extrajudiciais de Pernambuco", disponibilizado na plataforma Microsoft Forms (Anexo I) e durou entre 23 de maio e 30 de novembro de 2024.

Foram enviados 447 e-mails-convite (Anexo II) aos cartórios extrajudiciais cadastrados na base de dados do site Justiça Aberta do CNJ, com toda a explicação da pesquisa e contato em caso de dúvidas.

Ao todo, 25 cartórios extrajudiciais responderam à pesquisa. Desses, 25% pertencem ao Registro Civil das Pessoas Naturais, 22% ao Tabelionato de Notas, 18% ao Tabelionato de Protesto de Títulos, 18% ao Registro de Imóveis e 16% ao Registro de Títulos e Documentos e Civil das Pessoas Jurídicas.

Apesar dos esforços para coletar respostas, incluindo contatos por e-mail, mensagens por aplicativo de mensagem instantânea (Whatsapp), ligações telefônicas e visitas presenciais, um dos principais desafios enfrentados foi a resistência dos oficiais em participar da pesquisa, seja por falta de interesse ou dificuldade em compreender o tema abordado.

O formulário foi estruturado em duas partes: o primeiro bloco de perguntas (1 a 5) tem como objetivo identificar os cartórios extrajudiciais e responder de forma direta ao problema pde pesquisa, por meio de questões de resposta obrigatória. Já o segundo bloco (1 a 8) apresenta perguntas de caráter facultativo.

Perguntas:

1. Qual é o seu município de atuação?
2. O seu cartório se localiza na sede da comarca?
3. Qual é a atribuição do seu cartório?
4. Identifique o(s) serviço(s) de cloud computing (nuvem) utilizado(s) no cartório para realizar o backup do acervo digital. Em caso de utilização de mais de um serviço, por favor, indique todos.

5. Opções: Microsoft 365/Onedrive; Google Cloud Platform (GCP); Dropbox; iCloud; Amazon Web Services (AWS); IBM Cloud; Nuvem SERPRO "Nuvem do Governo"; Outra (especifique).
6. Existe um Centro de Processamento de Dados (CPD) isolado no seu cartório?
7. Você utiliza a versão corporativa/paga?
8. O servidor da nuvem utilizado está localizado no Brasil?
9. Se desejar fornecer informações adicionais, por favor, descreva-as abaixo.

A única resposta a nona pergunta foi: A dúvida é se há segurança para quando precisar usar localizar o acervo.

3 Resumo da Metodologia – Pesquisa Quantitativa

Forma de coleta dos dados	Questionário “Pesquisa Acadêmica sobre o Uso de Computação em Nuvem nos Cartórios de Pernambuco” disponibilizado no aplicativo Microsoft Forms
Duração da pesquisa	23 de maio a 30 de novembro de 2024
Convidados	447 cartórios de Pernambuco cadastrados na base de dados do site Justiça Aberta do CNJ
Respondentes	25 cartórios (aproximadamente 5,59%) Registro Civil das Pessoas Naturais: 25% Tabelionato de Notas: 22% Tabelionato de Protesto de Títulos: 18% Registro de Imóveis: 18% Registro de Títulos e Documentos e Civil das Pessoas Jurídicas: 16%

Fonte: Elaborado pela autora (2024).

4.3.2 Análise dos dados coletados

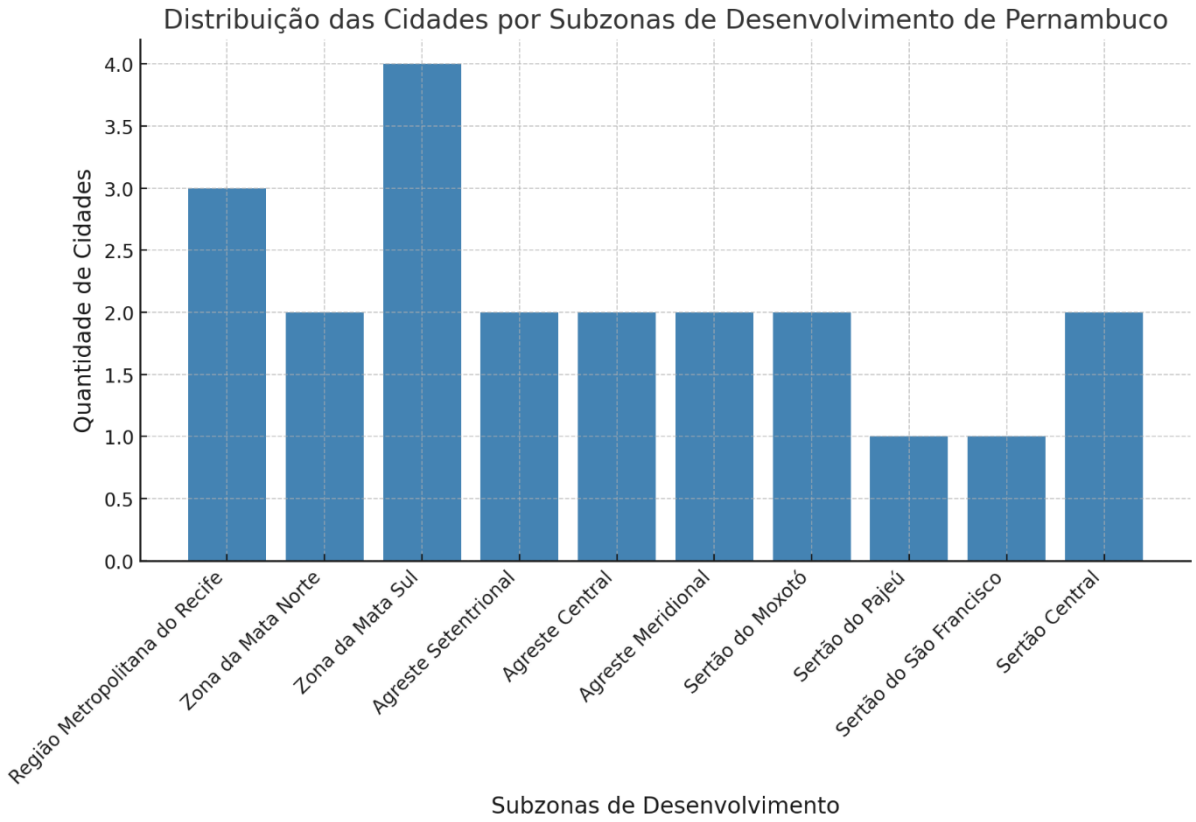
4.3.2.1 Municípios de atuação

A pesquisa contou com a resposta de 25 cartórios extrajudiciais em 22 municípios amplamente distribuídos por todo o estado de Pernambuco. A diversidade geográfica garante uma visualização, por amostragem, da realidade dos maiores municípios, como Recife,

Petrolina e Caruaru e dos menores, como Solidão e Vertente do Lério, pois todas as regiões engajaram (Região Metropolitana do Recife, Zona da Mata Sul, Zona da Mata Norte, Agreste Meridional, Agreste Setentrional, Agreste Central, Sertão do Moxotó, Sertão do São Francisco, Sertão Central e Sertão do Pajeú).

Todos os cartórios extrajudiciais respondentes: Amaraji; Angelim; Betânia; Bezerros; Caruaru; Casinhas; Goiana; Gravatá; Itaíba; Jaboatão dos Guararapes; João Alfredo; Manari; Palmares; Petrolina; Primavera; Quipapá; Recife; Salgueiro; São Caitano; Solidão; Verdejante; Vertente do Lério. O contraste dos níveis de maturidade da infraestrutura de tecnologia era esperado dentro do que já foi reconhecido pelo Provimento.

III Qual é o seu município de atuação?



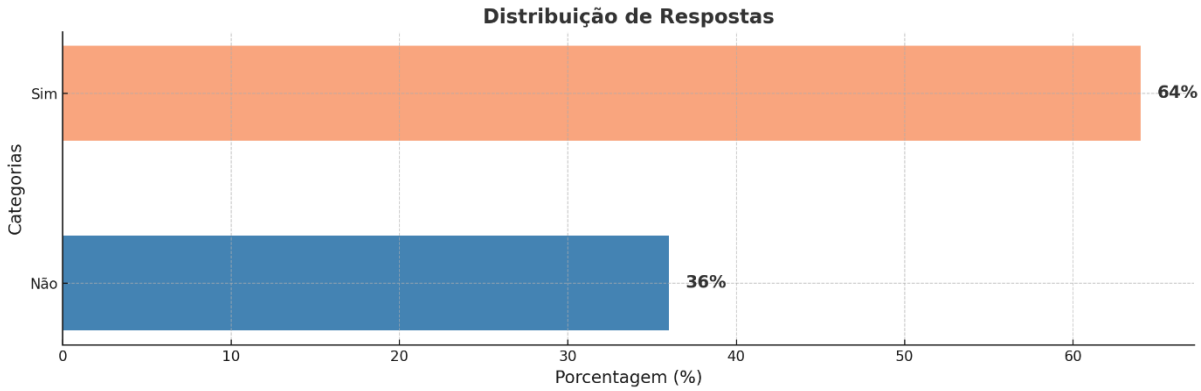
Fonte: Elaborado pela autora (2024).

4.3.2.2 Localização do cartório na sede da comarca

Após a promulgação da Lei Complementar nº 522/2023 da Assembleia Legislativa do Estado de Pernambuco (Alepe), que tem como objetivo "atualizar a organização do serviço extrajudicial do Estado de Pernambuco", várias serventias foram anexadas, extintas ou acumuladas, o que acabou influenciando na organização.

Diante dessa alteração, foi importante saber se o cartório estava de fato na comarca, o que se mostrou verdade para a maioria.

IV O seu cartório se localiza na sede da comarca?

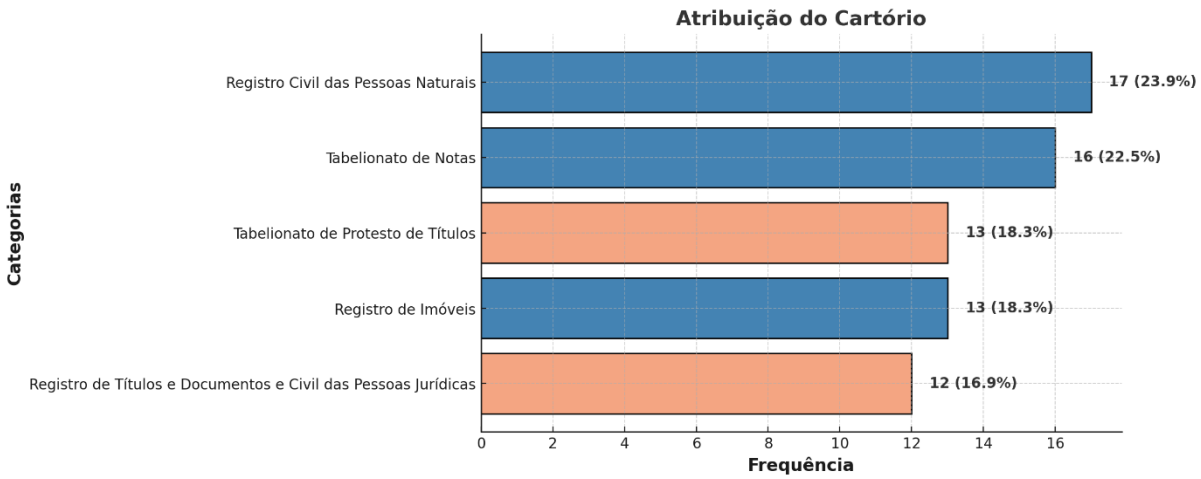


Fonte: Elaborado pela autora (2024).

4.3.2.3 Atribuição dos cartórios extrajudiciais

As atribuições estão bem distribuídas e abarcam todas as possibilidades descritas no art. 4º do Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco.

V Qual é a atribuição do seu cartório?



Fonte: Elaborado pela autora (2024).

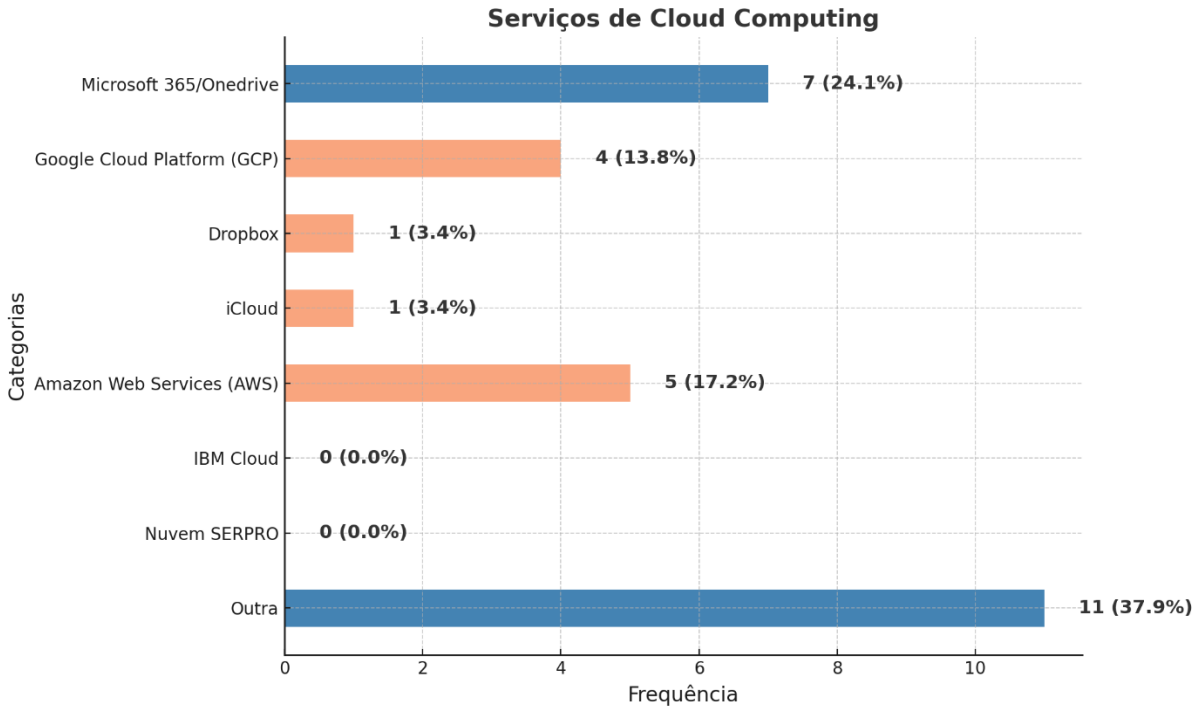
4.3.2.4 e 5 Serviços de computação em nuvem

Foram listadas seis nuvens (Microsoft 365/Onedrive; Google Cloud Platform (GCP); Dropbox; iCloud; Amazon Web Services (AWS); IBM Cloud; Nuvem SERPRO "Nuvem do Governo") e um campo aberto para descrição de outras. Cinco serviços de computação em nuvem foram indicados: Asgard; Consulticart; DeMaria; Fox Cloud; Fox Inline.

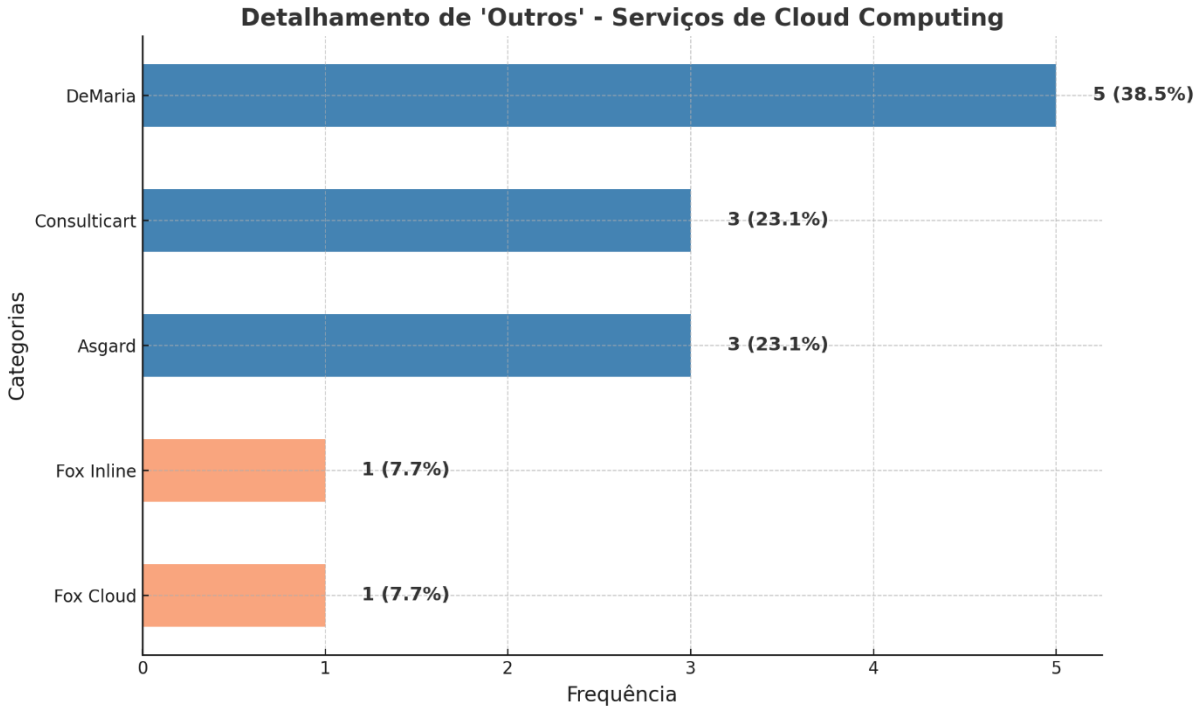
Em alguns casos existe a combinação do uso de nuvens, com as respostas: Amazon Web Services (AWS) + DeMaria; Google Cloud Platform (GCP) + DeMaria; Microsoft 365/Onedrive + iCloud; Fox Cloud + Fox Inline.

Destaca-se o uso de plataformas amplamente conhecidas, como Microsoft 365/OneDrive (23%) e Amazon Web Services (16%), porém, o percentual de "outros", que inclui provedores locais, como DeMaria (45% dos "Outros") e Consulticart (23%) é significativo. Estes provedores são nuvens especializadas para o serviço cartorário e extrajudicial brasileiro.

VI Identifique o(s) serviço(s) de cloud computing (nuvem) utilizado(s) no cartório para realizar o backup do acervo digital



Fonte: Elaborado pela autora (2024)



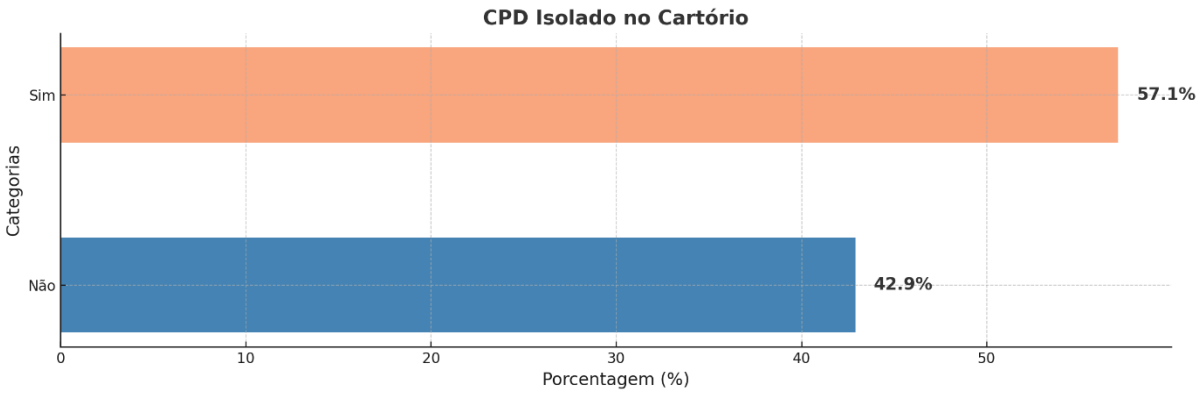
Fonte: Elaborado pela autora (2024)

4.3.2.6 Centro de Processamento de Dados (CPD)

O Local técnico (CPD) isolado é uma obrigatoriedade determinada pelo Art. 105, §1º, c do Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco que se aplica a todas as classes. Deve ser “isolada por parede de alvenaria ou divisória, dotada de refrigeração, porta com fechadura e acesso restrito aos funcionários da área de Tecnologia da Informação (TI)” (TJPE, 2023). Mais da metade dos respondentes (57%) relatou cumprir o requisito, enquanto 43% não contam com essa infraestrutura. A ausência de CPDs pode refletir limitações orçamentárias ou falta de capacitação técnica para implementação.

VII Existe um Centro de Processamento de Dados (CPD) isolado no seu cartório?

Fonte: Elaborado pela autora (2024).

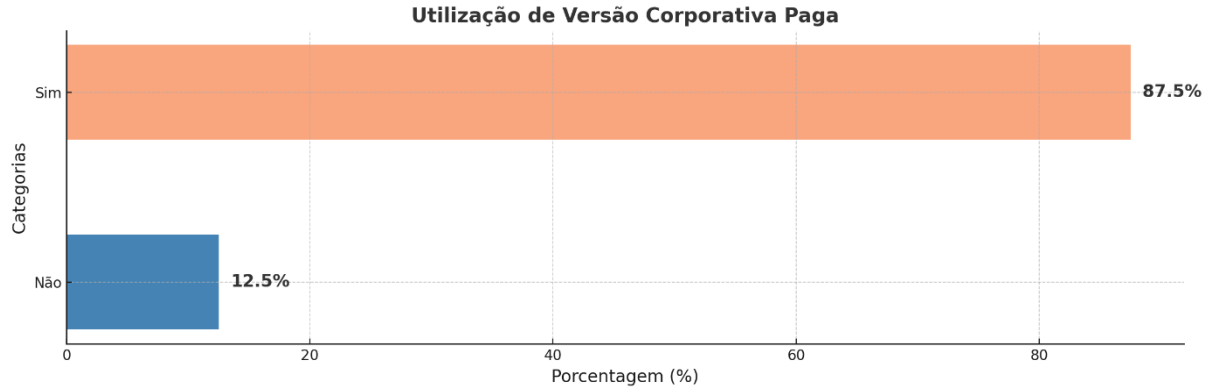


4.3.2.7 Utilização de versão corporativa/paga

O uso de software licenciado para uso comercial é obrigatório para todas as classes, como prescrito no Provimento nº74 em seu art. 6º, parágrafo único para que "todos os componentes de software utilizados pela serventia deverão estar devidamente licenciados para uso comercial, admitindo-se os de código aberto ou os de livre distribuição" (CNJ, 2018) e reiterado no art. 97 do Código de Normas.

Os resultados demonstram uma alta adesão (88%) ao padrão estabelecido, porém, aqueles que ainda não estão adequados criam uma insegurança na rede.

VIII - Você utiliza a versão corporativa/paga?



Fonte: Elaborado pela autora (2024).

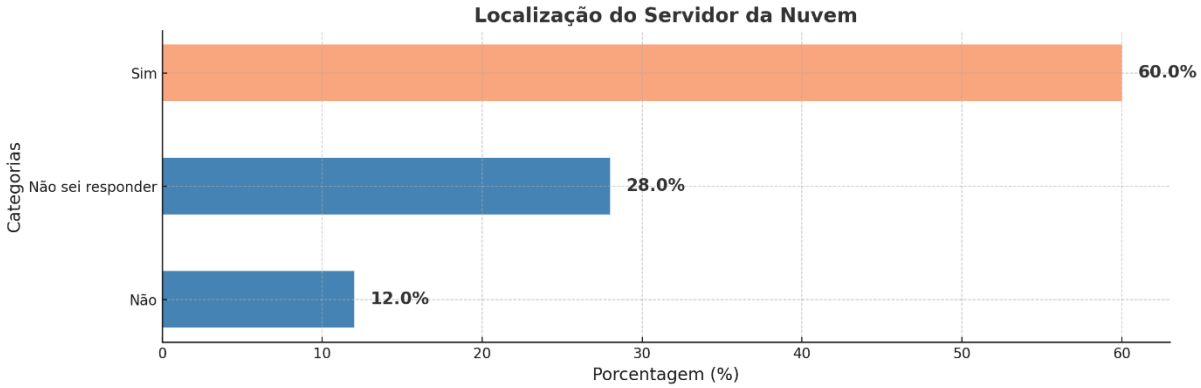
4.3.2.8 Localização do Servidor de Nuvem

A maioria dos respondentes utiliza servidores localizados no Brasil (65%), cumprindo o padrão estabelecido; ou pelo uso de empresas nacionais ou pela localização nacional do servidor da big tech contratada.

A presença de "Não sei responder" (22%) evidencia uma lacuna de conhecimento técnico, possivelmente indicando necessidade de capacitação ou clareza nos contratos de serviços. A única resposta formal coletada no formulário foi "a dúvida é se há segurança para quando precisar usar localizar o acervo", porém, durante as conversas de convite via Whatsapp alguns registradores manifestaram a preocupação por não saberem apontar objetivamente a localização física do servidor, especialmente em caso de correição.

Essa inquietação é legítima diante da determinação "os responsáveis pelas serventias extrajudiciais deverão atender às disposições da Lei Geral de Proteção de Dados, independentemente do meio ou do país onde os dados estão localizados (...)" presente no art. 79 do Provimento nº 149/2023.

IX O servidor da nuvem utilizado está localizado no Brasil?



Fonte: Elaborado pela autora (2024).

4.3 Arcabouço Jurídico

A pesquisa, ainda que por amostragem, levantou dados que são valiosos para o debate sobre o uso de serviço de computação em nuvem para realização de cópia de segurança e sua relação com a soberania de dados. Se, por um lado, evidenciou a preferência a provedores estrangeiros, sendo a Microsoft Corporation o mais utilizado, também trouxe a novidade da aderência a empresas nacionais, com menção a empresa paulista DeMaria e a pernambucana Consulticart, e os ocasionais usos combinados de provedores estrangeiros e nacionais.

Para que o trabalho não se limite à identificação do problema e viabilize a formulação de estratégias eficazes, é necessário verificar se a legislação brasileira contempla a proposta que será apresentada.

4.3.1 Constituição Federal

O Conselho Nacional de Justiça tem a prerrogativa de planejar, regulamentar e implementar as medidas que julgar necessárias. Essa competência está expressamente prevista na Constituição Federal, no art. 103-B, § 4º, incisos I e VII, que atribuem ao Conselho a responsabilidade pelo controle da atuação administrativa e financeira do Poder Judiciário. Além disso, cabe ao CNJ “expedir atos regulamentares, no âmbito de sua competência, ou recomendar providências” e no relatório anual, propor “as providências que julgar necessárias, sobre a situação do Poder Judiciário no País e as atividades do Conselho, o qual deve integrar mensagem do Presidente do Supremo Tribunal Federal a ser remetida ao Congresso Nacional(...)”.

4.3.2 Lei dos Cartórios

Em sequência, a Lei nº 8.935/1994, ou Lei dos Cartórios, em seu art. 38, estabelece que o "juízo competente zelará para que os serviços notariais e de registro sejam prestados com rapidez, qualidade satisfatória e de modo eficiente, podendo sugerir à autoridade competente a elaboração de planos de adequada e melhor prestação desses serviços(...)".

4.3.3 Regimento Interno do Conselho Nacional de Justiça

Segundo o site do Conselho Nacional de Justiça, "a eficiência dos serviços judiciais está relacionada à formulação e execução de políticas judiciárias, programas e projetos que promovam a modernização e a celeridade dos serviços dos órgãos do Judiciário(...)".

A Resolução nº 67/2009, o Regimento Interno do Conselho Nacional de Justiça, traz em seu art. 4º que o seu Plenário do Conselho Nacional de Justiça é responsável pelo controle da atuação administrativa e financeira do Poder Judiciário, zelar pela autonomia do Poder Judiciário e pela observância do Estatuto da Magistratura e possui a competência para expedir atos regulamentares dentro de sua esfera de atuação ou recomendar providências, conforme necessário (Brasil, 2009).

Vale mencionar que, embora o Regimento mencione inicialmente o "Poder Judiciário", posteriormente, inclui expressamente os "serviços auxiliares, serventias e órgãos prestadores de serviços notariais e de registro que atuem por delegação do poder público ou oficializados(...)".

Foi criada no âmbito da Corregedoria Nacional de Justiça por força do art. 3º do Provimento n. 134, de 24 de agosto de 2022, a Comissão de Proteção de Dados, de caráter consultivo, é responsável por propor, independentemente de provocação, diretrizes com critérios sobre a aplicação, interpretação e adequação das Serventias à LGPD, espontaneamente ou mediante provocação pelas Associações.

Na 13ª Sessão Ordinária da Comissão de Proteção de Dados do CNJ, o Diretor-Presidente da ANPD, Waldemar Gonçalves, demonstrou interesse em fazer um acordo de cooperação técnica com o CNJ para firmar uma agenda de colaboração. O juiz Fernando Tasso, do Tribunal de Justiça do Estado de São Paulo,

> Externou preocupação com relação à escala e à diversidade de fontes regulatórias que eventualmente possibilitem a entidades privadas, valendo-se de lacunas na legislação e de uma postura omissiva do poder público, obter o acesso a dados pessoais, atraindo assim a responsabilidade civil do Estado. (ATA N. 1809749).

4.3.4 Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco

Após a análise da legislação e atos normativos pertinentes, constata-se que art. 91 do Código de Normas abre o espaço para a fundamentação do plano de ação e amarra todas as possibilidades que serão apresentadas.

> Art. 91. Os sistemas, programas ou aplicativos de informática (*software*) utilizados e contratados na serventia são de livre escolha do delegatário e não dependem de autorização prévia ou especial da Corregedoria Geral da Justiça, devendo ser observados os requisitos e padrões tecnológicos e de segurança definidos pelo Provimento nº 74/2018 do Conselho Nacional de Justiça e alterações posteriores.
> Parágrafo único. O titular deve comunicar à Corregedoria Geral da Justiça, quando da implantação do sistema de informática, enviando cópia do respectivo contrato pelo Malote Digital:
> I – a identificação do sistema, programa ou software contratado, com a descrição detalhada dos seus aplicativos, recursos e capacidade de armazenamento;
> II – o nome da empresa ou profissional técnico contratado para o fornecimento, assistência técnica e desenvolvimento do sistema.

A autonomia de escolha do delegatário é garantida constitucionalmente e, por óbvio, esse princípio não está sob análise. Na verdade, o questionamento recai sobre a livre escolha "devendo ser observados os requisitos e padrões tecnológicos e de segurança definidos pelo Provimento nº 74/18", que não especifica de forma detalhada quais são os serviços de nuvem mais adequados para a contratação.

4.4 Projeto de Governança: Catálogo de Serviços de Nuvem em conformidade com parâmetros de segurança

O escopo do projeto é a realização de um estudo diagnóstico-propositivo que inventaria as nuvens contratadas para armazenar as cópias de segurança do acervo e consolida os dados a fim de permitir a realização de testes de segurança e conformidade.

O estudo é dividido em quatro etapas, sendo a primeira o levantamento dos serviços utilizados nos 549 cartórios extrajudiciais de Pernambuco, conforme declarado pelo TJPE; a segunda e terceira, análise de documentação e testes de segurança da informação; e a quarta, a consolidação dos dados para desenvolver um catálogo de provedores (a ser disponibilizado em lista homologada) conformidade com a legislação brasileira e os parâmetros internacionais de segurança da informação.

Para manter a objetividade e garantir um processo transparente e auditável, as fases devem ser contabilizadas através de sistema de pontuação com pesos diferentes; sempre com o princípio da primazia da soberania de dados em primeiro lugar.

4.4.1 1ª Etapa: Mapeamento extensivo dos provedores contratados

O *backup* não está concentrado em um só ambiente, como identificado no resultado da pergunta "4 - Identifique o(s) serviço(s) de *cloud computing* (nuvem) utilizado(s) no cartório para realizar o backup do acervo digital".

É possível verificar, para além das respostas coletadas, que os cartórios disponibilizam vários meios de contato, como a opção de mensagem pelo próprio site, e-mail e o número do WhatsApp, que é a plataforma de rede social mais utilizada no Brasil, com uma aderência de 93,4% entre os usuários de internet em 2023 (Statista, 2024). Apesar de ser uns meios de comunicações mais utilizados no país, em nenhum momento o WhatsApp foi mencionado.

Esse cenário indica uma pulverização do acervo e solicita uma listagem minuciosa das seguintes categorias:

i. Nuvem designada: o provedor principal utilizado para o armazenamento do acervo;
ii. Sistema operacional: as soluções nativas de sincronização, como iCloud e OneDrive, considerando o salvamento automático;
iii. Aplicativos de mensageria: WhatsApp, Telegram e outras plataformas que armazenam informações em nuvem;
iv. Servidores de hospedagem de sites: infraestrutura utilizada para hospedagem de sites institucionais, considerando o impacto da configuração do servidor no armazenamento de dados.

Deverá ser criado um fluxograma abrangendo as combinações mais frequentes para uma visão holística do ecossistema.

4.4.2 2ª Etapa: Inventário da Documentação e Classificação

Essa etapa é dividida em duas fases, a partir da listagem obtida, que consistem em:

I. Levantamento das seguintes informações (rol não exaustivo):
i. Avisos de Privacidade;
ii. Compromisso de Autonomia Digital;
iii. Contratos;

iv. Política de Cookies;
v. Políticas de Privacidade;
vi. Relatório de Privacidade ou Transparência;
vii. Termos e Condições;
viii. Demais Documentos Corporativos.

II. Análise (organizada em ciclos de examinação) da conformidade com a LGPD, o Código Nacional de Normas da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça – Foro Extrajudicial (CNN/CN/CNJ-Extra) e o Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco.

Essa etapa é classificatória e determinará a ordem de prioridade de avaliação técnica, a propósito, os provedores em conformidade seguirão para a próxima etapa; fica a critério da CGJ solicitar a documentação daqueles que estão inadequados.

Subfase facultativa: Levantamento dos custos médios dos serviços em nuvem para verificar viabilidade e custo-benefício para as Classes descritas no Provimento nº74/2018.

4.4.3 3ª Etapa: Teste de Segurança da Informação

Essa fase propõe-se a avaliar, por meio de testes de segurança da informação, todos os serviços de computação em nuvem, respeitando a ordem previamente estabelecida.

Devem ser realizados testes de penetração; análise de conformidade com normas internacionais, como as ISO/IEC 17789:2014; ISO/IEC 27017; ISO/IEC 5140:2024 e ISO 35.210; testes com foco no respeito à soberania, seguindo, por exemplo, os parâmetros do Anexo IV do estudo "Security & Resilience in Governmental Clouds"; localização física dos data centers dos servidores; e outros procedimentos relevantes.

Observando o princípio do contraditório, os provedores de serviço devem ser comunicados sobre o projeto, uma vez que esta é uma fase eliminatória da análise. Caso alguma nuvem seja considerada inapta, essa decisão deve ser motivada e apresentada na listagem.

4.4.4 4ª Etapa: Ranqueamento

A fase final consolida os resultados dos diagnósticos das etapas anteriores, apresentando uma lista com a indicação dos provedores homologados e a classificação dos demais de acordo com o nível de conformidade, destinada exclusivamente para consulta e publicidade. A listagem

deve ser periodicamente atualizada, principalmente diante de casos graves de incidentes de segurança que forem analisados e sancionados pela ANPD.

Os provedores do serviço de nuvem serão dispostos em um catálogo, oferecendo opções que atendam aos critérios de conformidade e segurança estabelecidos para fortalecer a segurança do ecossistema digital e permitir a livre escolha do delegatário.

4.4.4.5 Ecossistema próprio

Como demonstra o estudo "Estratégia para a implementação de política pública para atração de Data Centers" lançado em 2023 pela Agência Brasileira de Desenvolvimento Industrial (ABDI) em parceria com o Ministério do Desenvolvimento, Indústria, Comércio e Serviços lançou em 2023, fica claro que já existe a iniciativa do Governo Federal no tópico específico da infraestrutura de *data centes*, como o levantamento de custos de instalação e manutenção, o mapeamento da localização das principais empresas, indústrias, e órgãos que contratam serviços de data center, as projeções para o mercado de serviços etc.

Seria remisso não recomendar a criação de uma infraestrutura tecnológica dedicada ao acervo dos cartórios extrajudiciais, que atenda integralmente aos requisitos estabelecidos pelo Provimento nº 74/2018 e assegure a conformidade com os parâmetros de segurança da informação, incluindo a localização nacional dos *data centers* utilizados nos serviços de computação em nuvem.

Porém é desarrazoado sugerir apenas essa solução, visto que é custosa e demora para ser concretizada. Diante do cenário, essa sugestão é a longo prazo e depende de muitos fatores além do controle do Conselho Nacional de Justiças e demais órgãos fiscalizadores.

CONCLUSÃO

A metodologia heterogênia de pesquisa permitiu uma visão holística do Provimento nº74/2028 do CNJ ao focar no quesito cópia de segurança do acervo digital usando a lente da soberania de dados como antítese do colonialismo de dados experienciado no século XXI.

O referido ato administrativo tem como objetivo "uniformizar a manutenção de arquivos eletrônicos/mídia digital de segurança dos livros e documentos que compõem o acervo dos serviços notariais e de registro" e, de fato, criou importantes requisitos para resguardar a segurança do ecossistema cartorário. Porém, a lacuna deixada na ausência de orientação sobre quais são os provedores do serviço de computação em nuvem adequados para o cumprimento da disposição se mostra prejudicial.

O recorte dos cartórios extrajudiciais do registro civil foi especialmente relevante para confirmar que o banco de dados presente nesses cartórios é a base do ordenamento jurídico brasileiro, pois é através da formalização da identidade da pessoa humana que o Estado a reconhece em sua plenitude, do nascimento ao óbito.

A pesquisa quantitativa orientou todo o trabalho e trouxe o indicador que, da amostra recolhida, a Microsoft é a empresa mais utilizada; a pesquisa documental investigou a qualidade do serviço da aludida e identificou graves incidentes de segurança com lenta resolução no quesito de gerenciamento de crise, desta forma, também foi possível concluir que a percepção que as nuvens estrangeiras são mais seguras se mostra desconectada da realidade. Para além da familiaridade e pesquisas de marketing, existem problemas sérios de segurança não só tecnológica, mas para os Estados que as utilizam.

Através da pesquisa histórica-bibliográfica foi possível rever como a infraestrutura da computação e internet foi criada como arma de guerra pelos estadunidenses e assim permanece, como foi à público o escândalo do NSA Files que não só delatou a espionagem no mandato do então presidente Barack Obama via agências governamentais, como os acordos EUA-Inglaterra para interceptação de informações via cabos submarinos. É leviano negar que o espaço digital é um campo de batalha geopolítica.

De forma que a proteção dos dados pessoais do brasileiro é uma questão da garantia da manutenção do Estado brasileiro, que precisa da sua própria infraestrutura para evitar ataques, invasões, perda de arquivos, espionagem entre muitas outras ameaças de segurança.

A criação de data centers e servidores é um projeto custoso e que já está fase de desenvolvimento pelo Ministério do Desenvolvimento, Indústria, Comércio e Serviços; é importante frisar que já existem data centers e servidores no Brasil, e que o ponto principal desse trabalho é que exista servidores dedicados a máquina do Estado.

Para além da conclusão da necessidade da infraestrutura, é preciso desenvolver uma solução que possa funcionar a curto e médio prazo, que foi o apresentado “Projeto de Governança: Catálogo de Serviços de Nuvem em conformidade com parâmetros de segurança”. As quatro etapas seguem uma lógica de compliance aplicada ao contexto do serviço de nuvens, dividindo o projeto para a identificação de todas as nuvens utilizadas, uma verificação dupla da documentação jurídica e confiabilidade da segurança da informação dos serviços e, por fim, o ranqueamento das nuvens homologadas em lista para que os delegatários possam fazer uma escolha informada.

Como anteriormente descrito, a pesquisa quantitativa durou 6 meses e conseguiu atingir apenas 5,59% dos convidados. O seu ponto forte foi a distribuição geográfica dos respondentes e a variedade dos tipos de cartórios extrajudiciais, mas a amostra é insuficiente para criar um framework com indicadores precisos.

Recomenda-se, de forma institucional, a continuidade da pesquisa pelo Tribunal de Justiça de Pernambuco e a Corregedoria-Geral da Justiça de Pernambuco, porque a pesquisa foi realizada nesse estado. É possível que o TJPE não seja capaz de, sozinho, desenvolver toda a proposição, porém é factível solicitar suporte ao CNJ.

Esse projeto também não é simples de ser desenvolvido, porém é uma forma de preservar o acervo nacional, a segurança jurídica de todo o ordenamento e a autonomia do Brasil (ainda se mantém subordinado ao colonialismo tecnológico devido à sua dependência de empresas estrangeiras).

Recomenda-se que a execução do projeto considere o seguinte questionamento: até que ponto a guarda dos documentos de natureza pública pode ser confiada a empresas privadas do Norte Global, que não só tem um histórico colonialista, como comprovadas condutas de espionagem, corrupção, manutenção de oligopólio, processamento de dados pessoais para manipulação e interferência em outras democracias, inclusive a brasileira?

Em conclusão, o Brasil continua sofrendo as consequências do colonialismo que não acabou, apenas adicionou mais uma camada de exploração, porém, a luta pela autonomia de ser ramificada como a opressão foi enraizada no país.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD**). Guia de proteção de dados pessoais para o poder público. Versão final**. 2020. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 12 nov. 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD**). Resolução CD/ANPD nº 19, de 23 de agosto de 2024**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396. Acesso em: 5 dez. 2024.

AMAZON WEB SERVICES INC. **Contrato do Cliente AWS**. Disponível em: https://aws.amazon.com/pt/agreement/. Acesso em: 02 fev. 2023.

AMAZON WEB SERVICES INC. **Notificação de Privacidade.** Disponível em: https://aws.amazon.com/pt/privacy/. Acesso em: 02 fev. 2023.

AMAZON WEB SERVICES INC. **Termos de Serviço da AWS**. Disponível em: https://aws.amazon.com/pt/service-terms/. Acesso em: 02 fev. 2023.

ARAÚJO NETO, Reinaldo Juvino de; AGUIAR, Janderson Jason Barbosa. **Os impactos da Lei Geral de Proteção de Dados (LGPD) na segurança da informação: uma revisão da literatura.** Disponível em: http://doi.org/10.7769/gesec.v15i2.3442. Acesso em: 29 abr. 2024.

AWS. **What is cloud file storage?** Disponível em: https://aws.amazon.com/what-is/cloud-file-storage/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is cloud infrastructure?** Disponível em: https://aws.amazon.com/what-is/cloud-infrastructure/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is cloud storage?** Disponível em: https://aws.amazon.com/what-is/cloud-storage/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is data backup?** Disponível em: https://aws.amazon.com/what-is/data-backup/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is data store?** Disponível em: https://aws.amazon.com/what-is/data-store/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is database?** Disponível em: https://aws.amazon.com/what-is/database/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS**. What is hybrid cloud?** Disponível em: https://aws.amazon.com/what-is/hybrid-cloud/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is latency?** Disponível em: https://aws.amazon.com/pt/what-is/latency/. Acesso em: 18 nov. 2024.

AWS. **What is public cloud?** Disponível em: https://aws.amazon.com/what-is/public-cloud/?trk=faq_card. Acesso em: 20 nov. 2024.

AWS. **What is structured data?** Disponível em: https://aws.amazon.com/what-is/structured-data/?trk=faq_card. Acesso em: 20 nov. 2024.

AZAMBUJA, Darcy**. Introdução à ciência política.** 3. ed. Porto Alegre: Editora, 1979.

BBC. **Interesse dos EUA seria tecnologia do pré-sal, diz Fantástico.** 2013. Disponível em: https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilma_mm. Acesso em: 13 ago. 2024.

BELLOVIN, Steve. **Publicação em Mastodon.** Disponível em: https://mastodon.lawprofs.org/@SteveBellovin/111785021736568834. Acesso em: 13 ago. 2024.

BNDES. **BNDES lança linha de R$ 2 bilhões para data centers no Brasil.** Disponível em: https://agenciadenoticias.bndes.gov.br/detalhe/noticia/BNDES-lanca-linha-de-R$-2-bilhoes-para-data-centers-no-Brasil/#:~:text=O%20objetivo%20%C3%A9%20investir%20na,mais%20infraestruturas%20para%20essa%20finalidade. Acesso em: 9 out. 2024.

BORT, J. **How cloud computing evolved**. Tech Magazine, 2012.

BORTOLETO, Brayer Henrique; RIBEIRO, José Eduardo; FLORIAN, Fabiana. **Cloud computing para cartórios extrajudiciais.** Recima21 - Revista Científica Multidisciplinar, v. 3, n. 5, p. e351477, 2022. DOI: 10.47820/recima21.v3i5.1477. Disponível em: https://www.recima21.com.br/index.php/recima21/article/view/1477. Acesso em: 02 fev. 2023.

BOTACIM, Renato Sousa et al. **Computação nas nuvens: evolução e peculiaridade dos serviços e da segurança da informação**. Revista Interdisciplinar do Pensamento Científico (REINPEC), v. 2, n. 1, p. 259-269, 2016. Disponível em: https://www.researchgate.net/publication/309273851. Acesso em: 22 nov. 2024.

BRASIL**. Brasil encerra presidência rotativa do Conselho de Segurança da ONU**. Agência Brasil. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/202310/brasil-encerra-presidencia-rotativa-do-conselho-de-seguranca-da-onu. Acesso em: 02 abr. 2024.

BRASIL. Conselho Nacional de Justiça. **Altera o Código Nacional de Normas da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça – Foro Extrajudicial (CNN/CN/CNJ-Extra), instituído pelo Provimento n. 149, de 30 de agosto de 2023, para dispor sobre o registro do natimorto e para estabelecer o procedimento de promoção do registro de nascimento de criança ou adolescente no caso de omissão**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/5282. Acesso em: 13 nov. 2024.

BRASIL. Conselho Nacional de Justiça. **Resolução Nº 469, de 31 de agosto de 2022. Estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário.** Disponível em: https://atos.cnj.jus.br/atos/detalhar/4719. Acesso em: 16 maio 2024.

BRASIL. **Decreto nº 1, de 15 de novembro de 1889.** Disponível em: https://www2.camara.leg.br/legin/fed/decret/1824-1899/decreto-1-15-novembro-1889-532625-publicacaooriginal-14906-pe.html. Acesso em: 23 dez. 2024.

BRASIL. **Decreto nº 592, de 6 de julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos**. Diário Oficial [da] União, Brasília, 6 jul. 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto/1992/D0592.htm. Acesso em: 13 nov. 2024.

BRASIL. **Discurso da Presidenta da República Dilma Rousseff na abertura do debate geral da 68ª Assembleia Geral das Nações Unidas**. Disponível em:

https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/presidente-da-republica/presidente-da-republica-federativa-do-brasil-discursos/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas. Acesso em: 13 ago. 2024.

BRASIL. Governo Digital. **Compras de TIC**. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/compras-de-tic. Acesso em: 16 mai. 2024.

BRASIL. Governo Digital. **Contratações de TIC**. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic. Acesso em: 16 mai. 2024.

BRASIL. Governo Digital. **Modelo de Contratação de Software e Serviços em Nuvem.** Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/copy_of_legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem. Acesso em: 16 mai. 2024.

BRASIL. Governo Digital. **Portaria SGD/MGI nº 5.950 de 26 de outubro de 2023 - Modelo de contratação de software e de serviços de computação em nuvem.** Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/copy_of_legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023. Acesso em: 16 mai. 2024.

BRASIL**. Infraestrutura Nacional de Dados.** Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados. Acesso em: 16 mai. 2024.

BRASIL**. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 12 nov. 2024.

BRASIL. **Lei n.º 6.015, de 31 de dezembro de 1973. Dispõe sobre os registros públicos e dá outras providências.** Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6015original.htm. Acesso em: 12 nov. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;** altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1. Acesso em: 09 jul. 2024.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em: 11 out. 2022.

BRASIL. **Lei nº 8.935, de 18 de novembro de 1994. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8935.htm. Acesso em: 29 abr. 2024.

BRASIL. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. **Com diagnóstico inédito, governo começa a debater política nacional para data centers**. 2023. Disponível

em: https://www.gov.br/mdic/pt-br/assuntos/noticias/2023/junho/com-diagnostico-inedito-governo-comeca-a-debater-politica-nacional-para-data-centers. Acesso em: 9 out. 2024.

BRASIL. **Portaria SGD/ME nº 5.950, de 26 de outubro de 2023. Modelo de contratação de software e de serviços de computação em nuvem.** Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/copy_of_legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023. Acesso em: 16 maio 2024.

BRASIL. **Provimento nº 50, de 28 de setembro de 2015. Dispõe sobre a conservação de documentos nos cartórios extrajudiciais**. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/2512>. Acesso em: 29 abr. 2024.

BRASIL. **Provimento nº 74/ 2018 do CNJ nº 74, de 31 de julho de 2018. Dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil e dá outras providências.** Disponível em: <https://atos.cnj.jus.br/atos/detalhar/2637>. Acesso em: 29 abr. 2024.

BRASIL. **Relatório de Análise de Impacto Regulatório (RAIR)**. Disponível em: https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/copy_of_legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/relatorio-de-analise-de-impacto-regulatorio-rair-modelo-de-nuvem.pdf. Acesso em: 16 mai. 2024.

BRASIL. **Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte**. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 10 out. 2022.

BRASIL. **Resolução nº 469, de 31 de agosto de 2022. Estabelece diretrizes e normas sobre a digitalização de documentos judiciais e administrativos e de gestão de documentos digitalizados do Poder Judiciário.** Disponível em: https://atos.cnj.jus.br/atos/detalhar/4719. Acesso em: 16 mai. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 6.390, Distrito Federal. Relatora: Min. Rosa Weber. Requerente: Partido Socialismo e Liberdade (PSOL).** Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895176. Acesso em: 15 out. 2022.

CÂMARA DOS DEPUTADOS. **Lei Geral de Proteção de Dados Pessoais completa quatro anos com avanços e desafios.** Disponível em: https://www.camara.leg.br/noticias/904176-lei-geral-de-protecao-de-dados-pessoais-completa-quatro-anos-com-avancos-e-desafios/#:~:text=Embora%20tenha%20sido%20publicada%20em,aplicados%20h%C3%A1%20apenas%20um%20ano. Acesso em: 5 dez. 2024.

CÂMARA DOS DEPUTADOS. **Plataformização da educação e o ataque à soberania digital.** Disponível em: https://www.camara.leg.br/radio/programas/1106337-ep87-plataformizacao-da-educacao-e-o-ataque-a-soberania-digital/?pagina=10. Acesso em: 5 dez. 2024.

CÂMARA DOS DEPUTADOS. **Projeto de Resolução nº 821, de 2020.** Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1913985&filename=Tramitacao-RIC%20821/2020. Acesso em: 5 dez. 2024.

CARVALHO, José Murilo de**. Cidadania no Brasil: o longo caminho**. Disponível em: https://necad.paginas.ufsc.br/files/2012/07/CARVALHO-Jos%C3%A9-Murilo-de.-Cidadania-no-Brasil1.pdf. Acesso em: 5 dez. 2024.

CARVALHO, Julio Cesar; ALMEIDA, Tiago Henrique; MORAES, Martin Jose Fagonde. **Identificação das práticas de backup para segurança da informação de dados digitais de cartórios extrajudiciais registrais e notariais da região central de Curitiba no ano de 2018**. Disponível em: https://portaldeperiodicos.unibrasil.com.br/index.php/anaisevinci/article/view/4098. Acesso em: 29 abr. 2024.

CASSINO, J.F.; SOUZA, J.; SILVEIRA, S.A. (org). **Colonialismo de Dados: Como Opera a Trincheira Algorítmica na Guerra Neoliberal**. São Paulo: Autonomia Literária, 2021.

CETIC.BR. **Conectividade significativa: desafios e perspectivas no Brasil.** Disponível em: https://cetic.br/media/docs/publicacoes/7/20240415183307/estudos_setoriais-conectividade_significativa.pdf. Acesso em: 23 dez. 2024.

CHELLAPPA, R. K. **Intermediaries in Cloud-Computing: A New Computing Paradigm**. INFORMS Annual Meeting, Dallas, TX, October 26-29, 1997.

CILENTO FILHO, Oripide. **Como construir um data center adequado à sua empresa e à sua necessidade.** Disponível em: https://intrarede.nic.br/files/apresentacao/arquivo/1687/como%20construir%20um%20data%20center%20-%20parte-1.pdf. Acesso em: 20 nov. 2024.

CISCO. **Data Privacy Benchmark Study**. Cisco Trust Center. Disponível em: https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html. Acesso em: 14 abr. 2024.

CLOUDFLARE. **WannaCry ransomware: como o ataque afetou organizações em todo o mundo.** Disponível em: https://www.cloudflare.com/pt-br/learning/security/ransomware/wannacry-ransomware/. Acesso em: 12 nov. 2024.

CNJ. **Resolução nº 67, de 3 de março de 2009**. Disponível em: https://atos.cnj.jus.br/files/resolucao_comp_67_03032009_22032019151610.pdf. Acesso em: 23 dez. 2024.

CNN Business. **Google loses antitrust lawsuit in DOJ case**. Disponível em: https://edition.cnn.com/2024/08/05/business/google-loses-antitrust-lawsuit-doj/index.html. Acesso em: 13 ago. 2024.

CONGRESSO NACIONAL. **Projeto de Lei nº 5344, de 2013**. Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-5344-2013. Acesso em: 5 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **A atuação do CNJ ampliou atribuições e efetividade de cartórios extrajudiciais brasileiros**. Disponível em: https://www.cnj.jus.br/atuacao-do-cnj-ampliou-atribuicoes-e-efetividade-de-cartorios-brasileiros/. Acesso em: 5 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Ato Normativo nº 1733, de 5 de dezembro de 2024.** Disponível em: https://atos.cnj.jus.br/atos/detalhar/1733. Acesso em: 5 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Ato Normativo nº 3523, de 5 de dezembro de 2024**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3523. Acesso em: 5 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Ato Normativo nº 5696, de 5 de dezembro de 2024**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/5696. Acesso em: 5 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Comissão de Proteção de Dados da Corregedoria Nacional de Justiça**. Disponível em: https://www.cnj.jus.br/corregedoriacnj/extrajudicial/comissao-de-protecao-de-dados-da-corregedoria-nacional-de-justica/. Acesso em: 23 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Manual de digitalização**. 15 mar. 2023. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2023/03/proname-manual-digitalizacao-15-03-2023.pdf. Acesso em: 1 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Provimento nº 149, de 30 de agosto de 2023. Institui o Código Nacional de Normas da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça – Foro Extrajudicial (CNN/CN/CNJ-Extra).** Diário da Justiça Eletrônico do CNJ, n. 207, p. 7-242, 4 set. 2023. Disponível em: https://atos.cnj.jus.br/atos/detalhar/5243. Acesso em: 15 jan. 2025.

CONSELHO NACIONAL DE JUSTIÇA. **Provimento nº 47, de 18 de junho de 2015**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3265. Acesso em: 23 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Provimento nº 74, de 31 de julho de 2018. Dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados dos serviços notariais e de registro**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3523. Acesso em: 1 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Regulamento Geral da Corregedoria Nacional de Justiça**. Disponível em: https://www.cnj.jus.br/corregedoriacnj/regulamento-geral-da-corregedoria-nacional-de-justica/. Acesso em: 23 dez. 2024.

CONSELHO NACIONAL DE JUSTIÇA. **Seminário - A LGPD nos Cartórios extrajudiciais. 2023**. Palestra online, promovido pelo Conselho Nacional de Justiça (CNJ), 12 set. 2023. Disponível em: https://www.youtube.com/watch?v=bMY1yVQT7sw&t=3441s. Acesso em: 12 nov. 2024.

COULDRY, N.; MEJIAS, U.A. **The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism.** Stanford: Stanford University Press, 2019.

COUTO, Rodrigo S.; SECCI, Stefano; CAMPISTA, Miguel Elias M.; COSTA, Luís Henrique M. K. **Latência versus sobrevivência no projeto de centros de dados geograficamente distribuídos.** Disponível em: https://www.gta.ufrj.br/ftp/gta/TechReports/CSC14.pdf. Acesso em: 18 nov. 2024.

CVE DETAILS. **Vulnerability list for Microsoft.** Disponível em: https://www.cvedetails.com/vulnerability-list/vendor_id-26/Microsoft.html. Acesso em: 13 ago. 2024.

DONEDA, D. **Da Privacidade À Proteção De Dados Pessoais**. 2ª ed. São Paulo: Revista dos Tribunais, 2019.

ELECTRONIC FRONTIER FOUNDATION (EFF). **Globo - SATC**. Disponível em: https://www.eff.org/document/2013-09-03-globo-satc. Acesso em: 13 ago. 2024.

ENCYCLOPÆDIA BRITANNICA. **ARPANET.** Disponível em: https://www.britannica.com/topic/ARPANET. Acesso em: 4 dez. 2024.

E-NOTARIADO. **Customer.** Disponível em: https://www.e-notariado.org.br/customer. Acesso em: 1 dez. 2024.

EXAME. **Ex-funcionário da CIA acusa serviço de escutas britânico de ser pior que a NSA americana.** Disponível em: https://exame.com/mundo/ex-funcionario-da-cia-acusa-servico-de-escutas-britanico-de-ser-pior-que-a-nsa-americana/. Acesso em: 4 dez. 2024.

FERREIRA FILHO, Manoel Gonçalves. **Comentários à Constituição de 1988.** Saraiva, 1990.

FIGUEIREDO, Ruy. **Colonialismo de dados, descolonização da rede e infraestruturas de cabos submarinos: uma reflexão situada por prática artística.** Disponível em: https://doi.org/10.15448/1980-3729.2023.1.43590. Acesso em: 29 abr. 2024.

FOLHA DE S.PAULO. **Primeiro computador comercial do mundo completa 50 anos.** Folha Online. Disponível em: https://www1.folha.uol.com.br/folha/informatica/ult124u6520.shtml#:~:text=Univac%20%C3%A9%20a%20sigla%20de,pelos%20quais%20circulavam%20%C3%A1gua%20fria. Acesso em: 4 dez. 2024.

GOOGLE LLC. **Política de Privacidade do Google.** Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 02 fev. 2023.

GOOGLE LLC. **Termos de Serviço do Google.** Disponível em: https://policies.google.com/terms?hl=pt-BR. Acesso em: 02 fev. 2023.

GOVERNO FEDERAL. **Computação em nuvem**. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/computacao-em-nuvem. Acesso em: 5 dez. 2024.

GOVERNO FEDERAL. **Pregão Eletrônico SRP nº 18/2020 – Central de Compras.** Disponível em: https://www.gov.br/gestao/pt-br/assuntos/central-de-compras/transparencia/licitacoes/2020/pregao-eletronico-srp-no18-2020-central-de-compras. Acesso em: 5 dez. 2024.

HP. **Computer history: all about the ENIAC**. Disponível em: https://www.hp.com/ca-en/shop/offer.aspx?p=computer-history-all-about-the-eniac. Acesso em: 4 dez. 2024.

IBICT. **Computação em Nuvem**. Disponível em: https://livroaberto.ibict.br/bitstream/1/861/1/COMPUTA%c3%87%c3%83O%20EM%20NUVEM.pdf. Acesso em: 5 dez. 2024.

IBM. **Take a deep dive into the latest breach statistics and learn how to mitigate the risks.** Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 2 abr. 2024.

INFOMONEY. **Juiz dos EUA diz que Google violou leis de concorrência em mecanismos de busca.** Disponível em: https://www.infomoney.com.br/business/juiz-dos-eua-diz-que-google-violou-leis-de-concorrencia-em-mecanismos-de-busca/. Acesso em: 13 ago. 2024.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Estatísticas do registro civil.** Disponível em: https://www.ibge.gov.br/estatisticas/sociais/populacao/9110-estatisticas-do-registro-civil.html?=&t=sobre. Acesso em: 12 nov. 2024.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Estimativa do sub-registro**. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/populacao/26176-estimativa-do-sub-registro.html?=&t=noticias-e-releases. Acesso em: 12 nov. 2024.

INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT. **Cloud Computing: Challenges and Opportunities.** Disponível em: https://nimbusprof.com/wp-content/uploads/2019/06/ijnm_cloudcomputing.pdf. Acesso em: 5 dez. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION**. ISO/IEC 2382: Information technology — Vocabulary**. 1. ed. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:ed-1:v2:en. Acesso em: 10 mai. 2024.

ISO. International Organization for Standardization. I**nformação sobre Tecnologia da Informação - Código de categorização ICS 35.210.** Disponível em: https://www.iso.org/ics/35.210/x/. Acesso em: 16 maio 2024.

ISTOÉ DINHEIRO. **Lucro da Alphabet cresce 33,6% e atinge US$ 26,3 bilhões no 3º trimestre.** Disponível em: https://istoedinheiro.com.br/lucro-da-alphabet-cresce-336-e-atinge-us-263-bilhoes-no-3o-trimestre-2/. Acesso em: 4 dez. 2024.

JELLINEK, Gustav. **Teoría general del Estado**. Buenos Aires: Ed. Albatros, 1973.

JOVEM NERD. **Arquitetando a nuvem. Nerd na Cloud, episódio 1**, 15 jul. 2023. Disponível em: https://jovemnerd.com.br/podcasts/nerd-na-cloud/arquitetando-a-nuvem. Acesso em: 12 nov. 2024.

JOVEM NERD. **O templo de servidores dedicados e a história da nuvem.** Nerd na Cloud, episódio 3, 29 jul. 2023. Disponível em: https://jovemnerd.com.br/podcasts/nerd-na-cloud/o-templo-de-servidores-dedicados-e-a-historia-da-nuvem. Acesso em: 12 nov. 2024.

JOVEM NERD. **Tecnologia das nuvens para a ponta dos seus dedos.** Nerd na Cloud, episódio 2, 22 jul. 2023. Disponível em: https://jovemnerd.com.br/podcasts/nerd-na-cloud/tecnologia-das-nuvens-para-a-ponta-dos-seus-dedos. Acesso em: 12 nov. 2024.

LIMA, Eladio Lecey de; CRUZ, Eduardo Lopes da. **Soberania no direito internacional.** Disponível em: https://home.unicruz.edu.br/mercosul/pagina/anais/2015/1%20-%20ARTIGOS/SOBERANIA%20NO%20DIREITO%20INTERNACIONAL.PDF. Acesso em: 12 nov. 2024.

MADHAVAIAH, S.; BASHIR, A.; SHAFI, M. **The Cloud – Challenges and Issues.** The Cloud. Cambridge University Press, 24 set. 2019.

MEJIAS, U.A.; COULDRY, N. **Data grab: the new colonialism of big tech and how to fight back**. 1. ed. Londres: WH Allen, 2024.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing.** 2011. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-145/final. Acesso em: 02 fev. 2023.

MICROSOFT SECURITY RESPONSE CENTER (MSRC). **Results of major technical investigations for Storm-0558 key acquisition**. Disponível em: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/. Acesso em: 13 ago. 2024.

MICROSOFT. **Explore the globe of Microsoft datacenters**. Disponível em: https://datacenters.microsoft.com/globe/explore/. Acesso em: 20 nov. 2024.

MICROSOFT. **Política de Privacidade da Microsoft**. Disponível em: https://privacy.microsoft.com/pt-br/privacystatement?PrintView=true. Acesso em: 02 fev. 2023.

MICROSOFT. **Terms of Use.** Disponível em: https://www.microsoft.com/en-us/legal/terms-of-use. Acesso em: 02 fev. 2023.

MISHRA, Dhirendra. **Cloud Computing: The Era of Virtual World – Opportunities and Risks Involved**. International Journal of Computer Science and Engineering, v. 14, n. 3, p. 105. Disponível em: https://www.ijcse.net/docs/IJCSE14-03-04-105.pdf. Acesso em: 5 dez. 2024.

MISHRA, S. **Cloud computing: From concept to implementation**. IEEE Journal, 2014.

MORAES, Evaristo. **Extincção do Trafico de Escravos no Brasil.** 1ª ed. Rio de Janeiro: Biblioteca do Senado Federal, 1916.

MORDOR INTELLIGENCE. **Brazil Data Center Market - Growth, Trends, COVID-19 Impact, and Forecasts** (2024 - 2029). Disponível em: https://www.mordorintelligence.com/pt/industry-reports/brazil-data-center-market. Acesso em: 20 nov. 2024.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. **Clinton White House Archives: The ARPANET**. Disponível em: https://clintonwhitehouse4.archives.gov/WH/EOP/OVP/24hours/internet.html. Acesso em: 03 dez. 2024.

NIC.BR. **Computação na nuvem: a importância da conexão e da segurança.** Disponível em: https://nic.br/noticia/na-midia/computacao-na-nuvem-a-importancia-da-conexao-e-da-seguranca/. Acesso em: 5 dez. 2024.

NIC.BR. **Experiência em nuvem requer mais data centers e troca tecnológica.** Disponível em: https://nic.br/noticia/na-midia/experiencia-em-nuvem-requer-mais-i-data-centers-i-e-troca-tecnologica/. Acesso em: 5 dez. 2024.

NIC.BR. **O Brasil nas nuvens: o uso de serviços em nuvem nas organizações brasileiras**. Disponível em: https://www.nic.br/noticia/na-midia/o-brasil-nas-nuvens-o-uso-de-servicos-em-nuvem-nas-organizacoes-brasileiras/. Acesso em: 5 dez. 2024.

NIMBUS PROF. **Research**. Disponível em: https://nimbusprof.com/research/. Acesso em: 30 nov. 2024.

OLIVEIRA, Sérgio. **Espionagem britânica interceptou cabos de fibra ótica.** O Globo, 15 ago. 2014. Disponível em: https://oglobo.globo.com/mundo/espionagem-britanica-interceptou-cabos-de-fibra-otica-8773101. Acesso em: 03 dez. 2024.

ORACLE. **Saiba mais sobre a Nuvem Soberana da União Europeia da Oracle**. Disponível em: https://www.oracle.com/cloud/eu-sovereign-cloud/. Acesso em: 5 dez. 2024.

PAUPÉRIO, A. Machado. **O conceito polêmico de soberania**. 2. ed. rev. e ampl. Rio de Janeiro: Forense, 1958.

PERNAMBUCO. **Provimento nº 11/2023 – CGJ. Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco**. Disponível em:

https://portal.tjpe.jus.br/documents/29010/2155532/CÓDIGO+DE+NORMAS+COMPILADO+NOVO+-+15-12-2023.pdf/44f8b5d0-cf9e-5ee3-efdc-a401a1475301. Acesso em: 29 abr. 2024.

PINTO, Renata Ávila. **Soberania digital ou colonialismo digital?: novas tensões relativas à privacidade, segurança e políticas nacionais**. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/127003. Acesso em: 12 nov. 2024.

QUIJANO, Aníbal. **Colonialidade do poder, Eurocentrismo e América Latina**. In: LANDER, Edgardo (Org.). A colonialidade do saber: eurocentrismo e ciências sociais. Buenos Aires: CLACSO, 2005. Disponível em: http://bibliotecavirtual.clacso.org.ar/clacso/sur-sur/20100624103322/12_Quijano.pdf. Acesso em: 15 jun. 2022.

REDE NACIONAL DE ENSINO E PESQUISA (RNP). Disponível em: https://rnpmais.rnp.br/. Acesso em: 5 dez. 2024.

REUTERS. **Chinese hackers stole 60,000 emails from U.S. State Department in Microsoft hack - Senate**. Disponível em: https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/. Acesso em: 13 ago. 2024.

RICHTER, F. **Amazon leads $200-billion cloud market**. Disponível em: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/. Acesso em: 15 out. 2022.

ROBERTS, Larry. **The ARPANET and computer networks**. Introduction by Frank Kuo. Disponível em: https://dl.acm.org/doi/pdf/10.1145/61975.66916. Acesso em: 4 dez. 2024.

SCHMITT, Eric; WYDEN, Ron. **Senator Schmitt, Senator Wyden send letter to Department of Defense regarding continued use of singular vendor after series of concerning cybersecurity lapses.** Disponível em: https://www.schmitt.senate.gov/media/press-releases/senator-schmitt-senator-wyden-send-letter-to-department-of-defense-regarding-continued-use-of-singular-vendor-after-series-of-concerning-cybersecurity-lapses/. Acesso em: 13 ago. 2024.

SCORSIM, Ericson. **Cloud Computing: The Geopolitical and Geoeconomic Context.** Disponível em: https://direitodacomunicacao.com/br/cloud-computing-the-geopolitical-and-geoeconomic-context/. Acesso em: 29 abr. 2024.

SETO, Kenzo Soares. **Subimperialismo de dados: uma crítica ao colonialismo de dados diante das Big Techs sul-americanas**. Disponível em: https://periodicos.ufs.br/eptic/article/view/19199/14731. Acesso em: 29 abr. 2024.

SILVA, Fabiano Couto Corrêa da; PIRES, Thalia da Silva; WENDT, Lucas George. **Do colonialismo histórico ao colonialismo de dados.** Disponível em: https://doi.org/10.21728/logeion.2023v10n1.p75-90. Acesso em: 29 abr. 2024.

SILVA, José Afonso da. **Curso de direito constitucional positivo**.1994. p. 95.

SMITHSONIAN MAGAZINE. **The brief history of the ENIAC computer**. Disponível em: https://www.smithsonianmag.com/history/the-brief-history-of-the-eniac-computer-3889120/. Acesso em: 4 dez. 2024.

SOCRADAR. **Sensitive data of 65,000 entities in 111 countries leaked due to a single misconfigured data bucket**. Disponível em: https://socradar.io/sensitive-data-of-65000-

entities-in-111-countries-leaked-due-to-a-single-misconfigured-data-bucket/. Acesso em: 13 ago. 2024.

STATISTA. Leading social media platforms in Brazil 2023, by reach. Disponível em: https://www.statista.com/statistics/1307747/social-networks-penetration-brazil/. Acesso em: 5 fev. 2025.

STORCH, Julia. **Por que o Brasil é o principal destino Latam de data centers?** Exame, 1 jan. 2022. Disponível em: https://exame.com/bussola/por-que-o-brasil-e-o-principal-destino-latam-de-data-centers/. Acesso em: 20 nov. 2024.

Superior Tribunal de Justiça (STJ). **Acórdão de julgamento: Recurso Especial n.º 1.759.811 - SP.** Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/127003. Acesso em: 12 nov. 2024.

SUPREMO TRIBUNAL FEDERAL. **Ação Direta de Inconstitucionalidade nº 6387.** Disponível em: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf. Acesso em: 5 dez. 2024.

SUPREMO TRIBUNAL FEDERAL**. Decisão Liminar na ADI 6387**. Relatora: Ministra Rosa Weber. Disponível em: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf. Acesso em: 4 dez. 2024.

TAIT, Márcia M.; PERON, Alcides Eduardo dos Reis; SUÁREZ, Marcela. **Política Terrestre e corpo-território: dois conceitos para dar sentido ao colonialismo digital na América Latina**. Disponível em: https://doi.org/10.1080/25729861.2022.2090485. Acesso em: 29 abr. 2024.

TAVARES, Maria da Conceição. **Acumulação de capital e industrialização no Brasil**. 3ª Edição – Campinas/SP: UNICAMP, 1998.

THE GUARDIAN. **GCHQ taps fibre-optic cables for secret access to world's communications. 2013.** Disponível em: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Acesso em: 13 ago. 2024.

THE GUARDIAN. **NSA files: Decoded – what the revelations mean for you.** Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Acesso em: 13 ago. 2024.

THE NATIONAL WWII MUSEUM. **Scientific and technological advances of World War II**. Disponível em: https://www.nationalww2museum.org/war/articles/scientific-and-technological-advances-world-war-ii. Acesso em: 4 dez. 2024.

TRANSPARÊNCIA REGISTRO CIVIL**. Unknown death**. Disponível em: https://transparencia.registrocivil.org.br/unknown-death. Acesso em: 13 nov. 2024.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. Perguntas mais frequentes – Nascimento. Disponível em: https://www.tjdft.jus.br/informacoes/perguntas-mais-frequentes/extrajudicial/nascimento. Acesso em: 10 fev. 2025.

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO. **Código de Normas Compilado.** Disponível em: https://portal.tjpe.jus.br/documents/d/corregedoria/codigo-de-normas-compilado-novo-29-10-2024-pdf. Acesso em: 23 dez. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO. **Provimento nº 11/ 2023 – CGJ. Código de Normas dos Serviços Notariais e de Registro do Estado de Pernambuco.** Disponível em: https://portal.tjpe.jus.br/documents/29010/2155532/C%C3%93DIGO+DE+NORMAS+COMPILADO+NOVO+-+15-12-2023.pdf/44f8b5d0-cf9e-5ee3-efdc-a401a1475301. Acesso em: 29 abr. 2024.

TRIBUNAL DE JUSTIÇA DO ESTADO DE PERNAMBUCO. **Questionário Provimento nº 74 - CNJ**. Disponível em: https://portal.tjpe.jus.br/web/corregedoria/cartorios/cnj/questionario-provimento-74-cnj?p_l_back_url=%2Fweb%2Fcorregedoria%2Fbusca%3Fq%3Dprovimento%2B74. Acesso em: 6 nov. 2024.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 22 nov. 2024.

UNIÃO EUROPEIA**. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046. Acesso em: 5 dez. 2024.

UNIÃO EUROPEIA. **Diretriz 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046. Acesso em: 05 dez. 2024.

UNIÃO EUROPEIA**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 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 (Regulamento Geral sobre a Proteção de Dados - RGPD).** Disponível em: https://eur-lex.europa.eu/legal-

WHITE HOUSE. **The ARPANET, the precursor of today's Internet**. Disponível em: https://clintonwhitehouse4.archives.gov/WH/EOP/OVP/24hours/internet.html#:~:text=The%20ARPANET%2C%20the%20precursor%20of,function%20after%20a%20nuclear%20attack. Acesso em: 4 dez. 2024.

WIZ.IO. **38 terabytes of private data accidentally exposed by Microsoft AI researchers.** Disponível em: https://www.wiz.io/blog/38-terabytes-of-private-data-accidentally-exposed-by-microsoft-ai-researchers. Acesso em: 13 ago. 2024.

WIZ.IO. **Storm-0558 compromised Microsoft key enables authentication of countless Microsoft accounts.** Disponível em: https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr. Acesso em: 13 ago. 2024.

APÊNDICE A – Convite para a pesquisa

Outlook

Solicitação de Participação em Pesquisa de Mestrado - Prov. 74 CNJ

De Layla Leite <sampaioleite.layla@outlook.com.br>
Data Seg, 27/05/2024 15:00
Para 2rgi.olinda@gmail.com <2rgi.olinda@gmail.com>

Olá! Boa tarde, tudo bem?

Meu nome é Layla Sampaio Leite, sou mestranda em Direito, Justiça e Desenvolvimento pelo Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa – IDP. Estou realizando uma pesquisa para a minha dissertação, investigando qual é o serviço de nuvem que os cartórios de Pernambuco usam para fazer backup do acervo, conforme o Provimento nº 74 do CNJ. Coletar esses dados é essencial para entender onde o backup é feito, identificando as empresas mais frequentemente escolhidas para essa finalidade.

Você pode me ajudar respondendo a um breve formulário? São apenas 2 minutos do seu tempo! Clique no link para participar: https://forms.office.com/r/bZCVEjmKrF. Caso você prefira, abaixo está o QRCode de acesso.

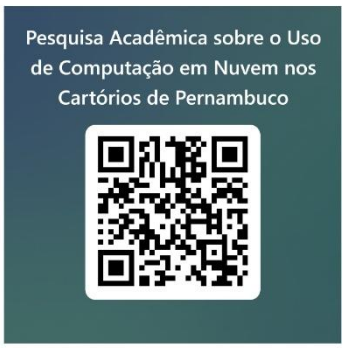
Sua contribuição é muito importante para garantir que os resultados sejam representativos e úteis para orientar possíveis políticas de armazenamento de dados e fortalecimento de infraestruturas nacionais de TI.

Desde já, muito obrigada pelo seu tempo e colaboração. Se tiver alguma dúvida, estou à disposição!

Atenciosamente,

Layla Sampaio Leite

--



APÊNDICE B – Formulário da Pesquisa

Pesquisa Acadêmica sobre o Uso de Computação em Nuvem nos Cartórios de Pernambuco

Olá!

Agradeço sua participação nesta pesquisa que integra minha dissertação de Mestrado Profissional em Direito, Justiça e Desenvolvimento pelo Instituto Brasileiro de Ensino, Pesquisa e Desenvolvimento (IDP).

Este estudo visa analisar qual é o serviço de computação em nuvem mais utilizado para fazer o backup do acervo pelos cartórios de Pernambuco, conforme o Provimento nº 74/2018 da Corregedoria Nacional de Justiça.

Todas as informações respondidas são confidenciais e destinam-se exclusivamente a fins acadêmicos.
A base de dados será anonimizada quando o processo de defesa da dissertação for concluído. Caso você tenha dúvidas ou queira fazer alguma solicitação, por favor, entre em contato pelo e-mail: sampaioleite.layla@outlook.com.br.

* Obrigatória

A seguir, encontram-se as perguntas fundamentais para a análise quantitativa.

Por favor, responda todas as perguntas dessa seção.

1. Qual é o seu município de atuação? *

2. O seu cartório se localiza na sede da comarca? *

- ◯ Sim
- ◯ Não

3. **Qual é a atribuição do seu cartório?** *

- ☐ Tabelionato de Notas
- ☐ Tabelionato de Protesto de Títulos
- ☐ Registro Civil das Pessoas Naturais
- ☐ Registro de Títulos e Documentos e Civil das Pessoas Jurídicas
- ☐ Registro de Imóveis

4. **Identifique o(s) serviço(s) de cloud computing (nuvem) utilizado(s) no cartório para realizar o backup do acervo digital. Em caso de utilização de mais de um serviço, por favor, indique todos.** *

- [ ] Microsoft 365/Onedrive
- [ ] Google Cloud Platform (GCP)
- [ ] Dropbox
- [ ] iCloud
- [ ] Amazon Web Services (AWS)
- [ ] IBM Cloud
- [ ] Nuvem SERPRO "Nuvem do Governo"
- [ ] Outra

5. Existe um Centro de Processamento de Dados (CPD) isolado no seu cartório? *

- ◯ Sim
- ◯ Não

As perguntas dessa seção não são obrigatórias, mas enriquecerão o estudo

6. Você utiliza a versão corporativa/paga?

- ◯ Sim
- ◯ Não

7. O servidor da nuvem utilizado está localizado no Brasil?

- ◯ Sim
- ◯ Não
- ◯ Não sei responder

8. Se desejar fornecer informações adicionais, por favor, descreva-as abaixo:

Este conteúdo não é criado nem endossado pela Microsoft. Os dados que você enviar serão enviados ao proprietário do formulário.

Microsoft Forms

ANEXO – Anexo IV Completo “Security & Resilience in Governmental Clouds”

Annex IV – List of threats

ID	Threat Description
Threats applicable to all the scenarios	
1.	Network breaks (temporary loss of routing components under assumption that this can be recovered)
2.	Traffic Loss
3.	Network management (ie, network congestion / mis-connection / non-optimal use, etc)
4.	Application interference (access to code – which is then subverted)
5.	CP administrator error
6.	Malicious insider (ineffective screening, ineffective logs, etc)
7.	Exhausted CP resources (losing performance)
8.	System overload, inability to scale
9.	Compromise of hypervisor or OS
10.	Social engineering attacks (impersonation – eg, security on demand)
11.	Data leakage on up/download, intra-cloud (sniffing, spoofing, man-in-the-middle attacks, side channel attacks, etc)
12.	Management interface compromise (manipulation, availability of infrastructure)
13.	Identity management system or provider (is point of failure for the system)
14.	DDoS
15.	DOS on another healthcare authority effecting yours
16.	Undertaking malicious probes or scans
17.	Modifying network traffic

ID	Threat Description
18.	Privileges escalation
19.	Theft of computer equipment
20.	Compromise or failure of the accounting and billing system
21.	Replay
22.	Guest-hopping (compartmentalisation)
23.	EHR service unavailability
24.	Other service unavailability
25.	Loss or compromise of EHR information
26.	Duplication of data
27.	Data inconsistency (ineffective data update)
28.	Loss or compromise of operational logs
29.	Loss or compromise of security logs (manipulation of forensic investigation)
30.	Interception of data during migration and periodic update of data in the cloud
31.	Compromise of data during migration and periodic update of data in the cloud
32.	Disasters (natural)
33.	Unauthorized access to premises (including physical access to machines and other facilities)
34.	Backups stolen
35.	Lost encryption keys
36.	Unsecure deletion of data (when requested by the patient)
37.	Loss of governance, control, specifications (SLA may be incomplete in covering all KPIs)
38.	Bankruptcy of cloud provider or cloud partner

ID	Threat Description
39.	Acquisition of cloud provider or cloud partner (increases likelihood of strategic shift and may put non-binding agreements at risk)
40.	Liability with respect to regulations (eg, notification of data security breaches to customers)
41.	Legal and data protection issues
42.	Conflicting privacy and security requirements
43.	Conflicts between regional or local guidelines – necessity to apply
Threats specific to the community cloud model and more in particular to the federated approach proposed in Reservoir project.	
44.	Billing service failure or reduced availability: the IaaS user requests his bill based on pay per usage. Any reduction in availability of the billing service will affect IaaS resilience.
45.	Reduced availability or failure of creating VEE (Virtual execution environments): setting up the VEE involves downloading the system images, instantiating then with the configuration parameters, starting them up, and creating the virtual network between the VEE. Any reduced availability in initiating VEE will affect IaaS resilience.
46.	Reduced availability or failure in shutting down VEE: deletes a VEE following an un-deployed request. Any reduced availability in shutting down VEE will impact IaaS resilience.
47.	Reduced availability or failure of the migration function: migration allows to relocate a VEE from one host to another without any service interruption. Any failure in the migration functionality will impact overall IaaS resilience.
48.	Reduced availability of the monitoring function: monitoring of VEE allows assessing the state of the infrastructure, and taking corrective actions if necessary, such as restarting, scaling or migrating VEE. Any reduced availability in the infrastructure monitoring will impact overall IaaS resilience.
49.	Billing service failure or reduced availability: the IaaS user requests his bill based on pay per usage. Any reduction in availability of the billing service will affect IaaS resilience.