UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DIR 2 - DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

JÚLIA ESCHER SEVERO

A TRANSFERÊNCIA E O ARMAZENAMENTO DE DADOS PESSOAIS EM SERVIDORES DE *CLOUD COMPUTING* NO EXTERIOR

PORTO ALEGRE
2023

JÚLIA ESCHER SEVERO

A TRANSFERÊNCIA E O ARMAZENAMENTO DE DADOS PESSOAIS EM SERVIDORES DE *CLOUD COMPUTING* NO EXTERIOR

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais na Universidade Federal do Rio Grande do Sul.

Orientador: Professor Doutor Fabiano Menke.

PORTO ALEGRE

2023

JÚLIA ESCHER SEVERO

A TRANSFERÊNCIA E O ARMAZENAMENTO DE DADOS PESSOAIS EM SERVIDORES DE *CLOUD COMPUTING* NO EXTERIOR

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais na Universidade Federal do Rio Grande do Sul.

Aprovado em: 11 de abril de 2023.

BANCA EXAMINADORA:

_____

Prof. Dr. Fabiano Menke
Orientador

_____

Prof. Dr. André Perin Schmidt Neto

_____

Mestranda Daniele Verza Marcon

AGRADECIMENTOS

Juntamente à correção de um trabalho final de física no Ensino Médio, enquanto estudava para as provas de vestibular, encontrei a seguinte frase: “se eu vi mais longe foi por estar sobre os ombros de gigantes”. A frase atribuída a Isaac Newton pode ter sido alterada em sua tradução ao longo dos anos, mas a sua essência permanece imutável: chegamos (e enxergamos) mais longe quando somos guiados por gigantes - e são a esses que atribuo os meus agradecimentos pelo presente trabalho e pela graduação que chega ao final.

Em primeiro lugar, agradeço aos meus pais, Luís Fernando Fleck Severo e Luciane Maria Escher Severo, pelo apoio incondicional que recebi durante toda minha vida. Sempre escutei os conselhos deles e a escolha pelo Direito, ademais de ter sido algo que decidi aos 9 anos de idade, foi um desses. Vocês não têm ideia do quanto os amo e agradeço diariamente por ter vindo a esse plano como filha de dois seres humanos tão incríveis. Obrigada por sempre terem confiado em mim e, antes de qualquer pessoa, terem acreditado no meu potencial. Se cheguei até aqui, em todos os sentidos, foi graças a vocês!

Estendo o agradecimento dos meus pais àqueles que os colocaram no mundo. Eu esperava ter pelo menos um deles nesse plano quando esse momento chegasse, mas todos partiram antes disso. De toda forma, agradeço imensamente pela família que vocês me permitiram usufruir. Apesar de todos os defeitos, eu não poderia ter sido mais abençoada. Em especial, homenageio minha avó Diva Boelhouwer, que não conseguiu alcançar a graduação em Direito, embora o tenha desejado imensamente, e meu bisavô Mainardo Pedro Boelhouwer, até então o único advogado e escritor da família: esse trabalho é pela memória de vocês.

Agradeço também à minha família de coração: Vera Lúcia da Silva, Melissa de Ávila Szortyka e Graziela da Silva de Ávila. Três mulheres incríveis que me amam desde antes de me conhecer. Vocês três fazem parte dessa conquista e estiveram comigo nos momentos prévios e posteriores a ela: meu muito obrigada por todo cuidado, amor e incentivo durante todos esses anos. Dinda Mel, logo será o teu trabalho de conclusão e espero estar contigo quando esse momento chegar. “Dinda” Grazi, obrigada por ter me acompanhado em tantos momentos, ter me oferecido a oportunidade de trabalhar contigo e de ser minha futura “madrinha” de Ordem.

Antes de agradecer ao meu orientador, Prof. Dr. Fabiano Menke, devo dizer que desde o segundo semestre da graduação, quando cursei a disciplina Parte Geral do Direito Civil, o desejei como tal. Professor, a sua trajetória acadêmica e profissional é objeto de inspiração para qualquer aluno. Me sinto imensamente honrada e realizada por contar com o teu apoio, incentivo e orientação durante meus anos na Faculdade de Direito da UFRGS, em especial, na

realização deste trabalho. A tua simplicidade, generosidade e tecnicidade são inigualáveis. Nesse momento, aproveito para dizer que a mais marcante de toda a minha graduação foi a disciplina que tive contigo, porque foi ela que me mostrou uma paixão, o Direito Civil. Com isso, afirmo que não há nada maior para um aluno do que ter um grande mestre ao seu lado: muito obrigada por ter sido o meu.

Estendo meu agradecimento a todos os demais professores da Faculdade de Direito da UFRGS. Embora tenha efetuado grande parte da graduação de forma remota, tenho certeza que a aluna e profissional que sou hoje tem influência de cada um deles. Ainda, em relação à Faculdade de Direito, agradeço a duas companheiras de graduação em especial: Juli Karin Arnold e Victória Catherine do Canto. Minhas parceiras de aulas e trabalhos remotos, bem como companheiras de gestão no Centro Acadêmico André da Rocha. Minha graduação foi mais leve graças a vocês!

Agradeço ainda a dois amigos que me acompanharam durante a escrita desse trabalho: João Vitor Berta Pires e Leonardo Santos Araújo. Ao primeiro, também conhecido como "meu melhor amigo", agradeço por ser e estar presente em todos os momentos da minha vida. Obrigada por acreditar em mim e nunca permitir que eu me sinta sozinha. Ainda vamos conquistar o mundo, mesmo que à distância. Por sua vez, ao segundo, meu grande colega de trabalho, com quem eu tenho a honra de compartilhar a semana, meu agradecimento mais que especial. Sem as nossas conversas, eu sequer teria escolhido o tema do meu trabalho. Espero que a nossa parceria siga além da Bem Promotora, porque nossa amizade vai muito além das obrigações trabalhistas.

Por fim, deixo meu agradecimento a todos aqueles que, embora não mencionados diretamente, sabem da importância que tiveram na minha jornada. Seja com palavras de carinho, incentivo ou apenas boas risadas, cada pequeno gesto faz parte desse trabalho. A todos, meus mais sinceros agradecimentos. Sem cada um de vocês, eu não teria chegado até aqui. De alguma forma, esse trabalho é resultado do impacto que cada um tem na minha vida. Eu não seria quem sou sem o apoio e carinho de cada um.

Aos meus pais, Luís Fernando Fleck Severo e Luciane Maria Escher Severo, que nunca pouparam esforços para que eu conquistasse os meus sonhos. Esse trabalho foi escrito por mim, mas sem vocês ele não existiria – assim como eu.

RESUMO

O presente estudo tem por objetivo analisar uma eventual possibilidade de minimizar os riscos envolvidos nas operações de transferência e armazenamento de dados pessoais relacionados a brasileiros em servidores internacionais de *cloud computing*. Por meio do método dedutivo de abordagem, utilizando-se da pesquisa bibliográfica como método de procedimento, as hipóteses levantadas são, por um lado, que a minimização de riscos é um procedimento viável, visto a previsão de circunstâncias para tanto no artigo 33 da Lei Geral de Proteção de Dados (LGPD) e, por outro, que a minimização de riscos não é plausível, devido à natureza da operação. Para responder à questão, optou-se pela divisão do trabalho em dois capítulos. O primeiro capítulo aborda a tecnologia da computação em nuvem, detalhando a sua origem, desenvolvimento e aplicabilidade, principalmente no que concerne aos riscos da operação. Por sua vez, o segundo capítulo versa sobre a maneira pela qual o assunto é tratado pelo Direito, mediante o debate legislativo sobre a transferência e armazenamento de dados pessoais relacionados a brasileiros em servidores internacionais de *cloud computing*. Por fim, concluiu-se pela hipótese da possibilidade de minimização dos riscos envolvidos nessa operação, por meio da definição e aplicação de critérios minuciosos, que devem ser controlados e fiscalizados pelos controladores e pela Autoridade Nacional de Proteção de Dados (ANPD).

Palavras-chave: Transferência e armazenamento de dados pessoais. Sistema de *cloud computing*. Proteção de dados pessoais.

ABSTRACT

The present study aims to analyze a potential possibility of minimizing the risks involved in the transfer and storage of personal data related to Brazilians in international cloud computing servers. Through the deductive method of approach, using the bibliographical research as a method of procedure, the hypotheses raised are, on the one hand, that the minimization of risks is a viable procedure, given the provision of circumstances for such in Article 33 of the General Law of Data Protection (Lei Geral de Proteção de Dados - LGPD) and, on the other hand, that the minimization of risks is not plausible, due to the nature of the operation. To answer the question, it was decided to divide the paper into two chapters. The first chapter addresses the cloud computing technology, detailing its origin, development, and applicability, especially regarding the risks of the operation. In turn, the second chapter deals with the way the subject is dealt with by Law, through the legislative debate on the transfer and storage of personal data related to Brazilians in international cloud computing servers. Finally, it was concluded that it is possible to minimize the risks involved in this operation, by defining and applying detailed criteria, which should be controlled and monitored by the controllers and by the Brazilian Authority for Data Protection (Autoridade Nacional de Proteção de Dados - ANPD).

Keywords: Transfer and storage of personal data. Cloud computing system. Protection of personal data.

LISTA DE ABREVIATURAS

Art.	Artigo
ANPD	Autoridade Nacional de Proteção de Dados
CC	Código Civil
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
EDPB	*European Data Protection Board*
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados
nº.	Número
p.	Página

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O fenômeno da globalização trouxe vantagens às sociedades modernas em igual proporção aos desafios. Em que pese o encurtamento das distâncias oportunizado pelos avanços tecnológicos e, em particular, o advento da internet, tenham favorecido o desenvolvimento econômico, político e social de diversas nações, as problemáticas decorrentes desse feito não foram poucas: a disponibilização e a livre circulação de dados pessoais é uma delas.

Embora a temática dos dados pessoais esteja em voga no país nos últimos anos, principalmente com a promulgação da Lei Geral de Proteção de Dados (LGPD), a Lei nº 13.709, de 14 de agosto de 2018[1], a preocupação da população brasileira com a exposição e tratamento de dados pessoais na internet ainda não é de ampla maioria, de acordo com pesquisa realizada pelo Comitê Gestor da Internet no Brasil (CIG)[2], visto que apenas 56% dos entrevistas deixaram de utilizar algum serviço ou plataforma na Internet por conta da preocupação com seus dados. Nessa perspectiva, é importante mencionar que a exposição dessas informações em diversas mídias é algo cotidiano, como ocorre, por exemplo, com a realização de compras em sites ou aplicativos.

O fenômeno da ampliação no uso e, consequentemente, coleta de dados pessoais, conhecido como *big data*, demonstra que cada vez mais indivíduos estão conectados, de modo que a onipresença dos dispositivos móveis na cotidiano faça com que o tratamento de dados seja inevitável, bem como a criação de novas formas de armazenamento e gestão dessas informações. Nesse sentido, os serviços de nuvem entram como aliados dos mais diversos usuários. Nas palavras de Anne S. Y. Cheung e Rolf. H. Weber,

> A nuvem nos permite acessar nossos documentos, fotos e arquivos de vídeo de qualquer lugar do mundo. Muitos de nós somos clientes da Dropbox e do Google, entre outros provedores de serviços na nuvem. Seja na busca on-line, no fluxo de mídia ou no WhatsApping, estamos todos na nuvem. Além disso, muitas empresas adquiriram recursos de computação através de provedores de serviços de nuvem em vez de adquirirem seus próprios ativos físicos de TI.[3] (tradução livre)

---

[1] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). DF: Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 mar. 2023.

[2] NÚCLEO de Informação e Coordenação do Ponto BR [edit.]. **Privacidade e proteção de dados pessoais 2021**: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 27 mar. 2023.

[3] A tradução livre é oriunda do seguinte texto original: "*The cloud allow us to access our documents, photos, and video files from anywhere in the world. Many of us are customers of Dropbox and Google, amongst other cloud service providers. Be it online searching, media streaming or WhatsApping, we are all in the cloud. In addition, many businesses have purchased computing resources through cloud service providers rather than acquiring*

Sendo assim, os sistemas de *cloud* se mostram eficientes tanto para as empresas, sejam elas públicas ou privadas, como para o usuário individual, que é o titular dos dados pessoais. No que concerne ao setor empresarial, muitas empresas encontraram no *cloud computing* a melhor solução para a manutenção e retenção de dados pessoais dos consumidores e das próprias companhias. Sendo assim, os dados podem ficar retidos em servidores internacionais, como ocorre com a Amazon Web Services (AWS), Google Cloud Platform (GCP) e Microsoft Azure, líderes em serviços de computação em nuvem[4], e que, em sua maioria, possuem servidores no estrangeiro.

Inúmeros são os artigos disponibilizados na Internet que apontam a segurança dessa tecnologia[5], bem como os certificados que cada plataforma possui atestando a sua confiabilidade. No entanto, não são raros os episódios de vazamentos de dados e exclusão ou perda de informações, problema que não se limita ao *cloud computing*. Sendo assim, apesar das diversas vantagens que o setor de informática é capaz de fornecer, os riscos envolvendo essas operações podem se tornar um obstáculo na sua aplicação, principalmente quando esses perigos são inerentes à atividade, como ocorre na transferência internacional de dados.

Nesse sentido, esse trabalho visa responder à seguinte pergunta: é possível minimizar os riscos envolvidos nas operações de transferência e armazenamento de dados pessoais nacionais em servidores internacionais de *cloud computing*? As hipóteses possíveis são duas: i) a minimização de riscos é um procedimento viável, visto que a própria Lei Geral de Proteção de Dados (LGPD) prevê, em seu art. 33, as circunstâncias em que a transferência pode ocorrer; e ii) a minimização de riscos não é plausível, devido ao fato das operações de transferência e armazenamento de dados pessoais serem, por natureza, uma operação arriscada.

O objetivo desta monografia é, portanto, verificar a possibilidade de minorar os riscos existentes nos procedimentos de transferência e armazenamento de dados pessoais nacionais em servidores estrangeiros de *cloud computing*, mesmo quando localizados em território nacional. O método de abordagem elencado para solucionar o problema é o dedutivo, visando

---

their own physical IT assets." (CHEUNG, Anne S. Y.; WEBER, Rolf H. (orgs.). **Privacy and Legal Issues in Cloud Computing**. Cheltenham: Edward Elgar Publishing, 2016. p. 1).

[4] COHEN, Jason. 4 Companies Control 67% of the World's Cloud Infrastructure. **PCMag**, 2021. Disponível em: https://www.pcmag.com/news/four-companies-control-67-of-the-worlds-cloud-infrastructure. Acesso em: 27 mar. 2023.

[5] Nesse sentido, pode-se exemplificar a questão com dois artigos que tratam sobre a segurança do sistema de *cloud computing*, os quais se encontram nos seguintes links: <https://thesciencebehindit.org/how-secure-is-data-stored-in-the-cloud/#:~:text=Data%20in%20the%20cloud%20can,computer%20connected%20to%20the%20Internet> e <https://us.norton.com/blog/privacy/cloud-data-security>.

analisar o contexto geral para resolver um problema específico. Ademais, o método de procedimento é essencialmente a pesquisa bibliográfica, com o intuito de investigar textos doutrinários e legislativos que possam, com base no objetivo, responder o problema de pesquisa.

No que tange ao escopo escolhido para o presente trabalho, optou-se pelo Direito Civil, visto que a regulação da proteção de dados vem sendo uma atribuição desse campo do Direito, em especial no que concerne aos direitos da personalidade, embora a matéria possua abrangência a outras áreas. Por sua vez, o método de divisão do trabalho escolhido foi o francês, com dois capítulos subdivididos em dois subcapítulos. Na primeira parte, tratar-se-á sobre questões atinentes à tecnologia do *cloud computing*, aplicando-se ênfase nos riscos da sua operação, que é o objeto da presente pesquisa. Nesse sentido, o primeiro subcapítulo versará sobre o desenvolvimento, a arquitetura e as formas de utilização da computação em nuvem, o que servirá de base para o subcapítulo seguinte, que tratará sobre a problemática acerca dessa tecnologia, mediante a comparação entre dois sistemas de computação: a computação local e a computação em nuvem.

A segunda parte, a seu turno, abrangerá a questão da transferência e armazenamento internacional de dados pessoais. No primeiro subcapítulo serão tratados os enquadramentos legais atinentes à Lei Geral de Proteção de Dados (LGPD), bem como uma comparação legislativa com a General Data Protection Regulation (GDPR), que é tida como a legislação mais avançada no que concerne à proteção de dados, bem como foi a regulamentação que inspirou os legisladores brasileiros. O segundo subcapítulo irá revisitar os riscos relacionados à transferência e armazenamento dos dados pessoais, visando a solucionar a problemática basilar do presente trabalho mediante a análise do sistema de *cloud computing* em relação às previsões da LGPD atinentes à transferência internacional de dados.

2 A TECNOLOGIA DO *CLOUD COMPUTING*

De acordo com o site da Amazon Web Services (AWS), líder do mercado de computação em nuvem no mundo[6], o *cloud computing* é a entrega de recursos de TI sob demanda por meio da internet com definição de preço de pagamento conforme o uso, sendo uma ferramenta amplamente utilizada nos dias atuais, principalmente durante o período pandêmico vivido nos últimos anos[7]. Em 2011, o National Institute of Standards and Technology (NIST) publicou uma recomendação com a definição do *cloud computing*:

> A computação em nuvem é um modelo que permite o acesso conveniente e sob demanda a um conjunto compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser provisionados e liberados rapidamente com um esforço mínimo de gerenciamento ou interação com o provedor de serviços.[8] (tradução livre)

No entanto, a construção do conceito de *cloud computing* não é uma tarefa simples, principalmente quando se está a regular essa atividade. Acerca do tema, o Parecer 05/2012 do Grupo de Trabalho para a Proteção de Dados (WP29), instituído pelo art. 29 da Diretiva 95/46/CE da União Europeia criou a seguinte definição:

> A computação em nuvem consiste num conjunto de tecnologias e modelos de serviços centrados na utilização e fornecimento via Internet de aplicações informáticas, de capacidade de tratamento e armazenamento e de espaço de memória. A computação em nuvem pode gerar importantes benefícios económicos, uma vez que os recursos a pedido podem ser com bastante facilidade configurados, alargados e acedidos via Internet.[9] (tradução livre)

---

[6] COHEN, Jason. 4 Companies Control 67% of the World's Cloud Infrastructure. **PCMag**, 2021. Disponível em: https://www.pcmag.com/news/four-companies-control-67-of-the-worlds-cloud-infrastructure. Acesso em: 27 mar. 2023.

[7] ESPECIALISTAS Inmetrics. Cloud Computing: como a pandemia acelerou a implementação. **Inmetrics**, [202?]. Disponível em: https://inmetrics.com.br/blog/cloud-computing-como-a-pandemia-acelerou-a-implementacao/. Acesso em: 27 mar. 2023.

[8] A definição original informa que "*cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*". Para mais informações, ver: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[9] O conceito original prevê o que segue: "*Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily*". O Parecer pode ser encontrado em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

No Brasil, em meados de 2013, foi apresentado um Projeto de Lei de iniciativa do Deputado Ruy Carneiro[10], que dispunha "sobre as diretrizes gerais e normas para a promoção, desenvolvimento e exploração da atividade de computação em nuvem no país". No entanto, o projeto não teve seguimento, de modo que não há nenhuma legislação específica sobre o assunto no Brasil. Nesse Projeto, o PL nº 5.344/2013, a definição de *cloud computing* era a seguinte:

> Art. 1º, § 1º – A computação em nuvem é definida como a exploração da atividade de tratamento, armazenamento, guarda e depósito virtuais, por sistemas eletrônicos ou eletromagnéticos e mediante contrato oneroso ou gratuito, no qual o depositário recebe informações, sistemas, programas, plataformas, ou qualquer espécie de dados do depositante ou titular, sejam codificados ou não, considerados conteúdo ou bens, (...)

A partir dessas definições, entende-se que a computação em nuvem vai além de uma alternativa ao armazenamento de arquivos em dispositivos de armazenamento ou discos rígidos: trata-se de uma ferramenta que permite a disponibilização de recursos de computação sob demanda. Nesse sentido, o *cloud computing* permite que o usuário acesse um sistema completo de TI de qualquer lugar do mundo, desde que tenha acesso à internet, sendo esta uma das maiores vantagens da sua utilização. Sendo assim, a computação em nuvem é uma vasta rede de servidores que se encontram remotamente conectados pelo mundo, operando em um único ecossistema.

No entanto, a computação em nuvem agrega, assim como diversas outras tecnologias, diversas polêmicas, em especial no que toca aos riscos da sua aplicação. Por ser uma ferramenta relativamente nova, é compreensível que haja uma apreensão no seu uso, embora seja uma tecnologia amplamente disseminada. Ademais, as questões atinentes a essa ferramenta envolvem conceitos alheios ao Direito, visto que se trata de uma operação informática, os quais serão explicados no decorrer desse capítulo. Em um contexto globalizado e interdisciplinar, como o que vivemos atualmente, o estudo desse mecanismo se mostra de suma importância, visto que os dados se encontram disponíveis em qualquer lugar do mundo.

---

[10] A íntegra do Projeto de Lei em questão pode ser encontrada em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=9D2469DC4935811455484A5873AE1673.proposicoesWeb2?codteor=1083767&filename=Avulso+-PL+5344/2013.

2.1 O DESENVOLVIMENTO E A ARQUITETURA DA COMPUTAÇÃO EM NUVEM

Embora o termo *cloud computing* tenha sido utilizado pela primeira vez em 1997 durante uma palestra acadêmica do professor de sistemas de informação Ramnath Chellappa[11], o método surgiu em meados da década de 1950. Na década de 1960, a computação em nuvem ganhou robustez com dois especialistas da área: John McCarthy e Joseph Carl Robnett Licklider. McCarthy, que ficou conhecido como o "pai da inteligência artificial" e foi o inventor da programação Lisp[12], tratou sobre o uso compartilhado do computador, de forma simultânea, por dois ou mais usuários; enquanto Licklider ajudou a desenvolver a Rede de Agências de Projetos de Pesquisa Avançada (ARPANET), que foi a primeira rede que permitiu o compartilhamento de informações entre computadores que não se encontravam no mesmo local.

O objetivo do pesquisador com a ARPANET era possibilitar a conexão em qualquer lugar e a qualquer horário, pontos que são tidos como pilares basilares da computação em nuvem: a disponibilidade e a acessibilidade. No entanto, durante esse período, o mecanismo era de difícil acesso, visto que o maquinário era extremamente caro e escasso na maioria das organizações. Dessa forma, a tecnologia do *cloud computing* passou a ser utilizada em larga escala quando disponibilizada comercialmente por grandes marcas, como a Amazon e o Google, o que ocorreu somente nos anos 2000.

Como dito anteriormente, a nuvem consiste em mecanismo que permite o acesso aos mais diferentes tipos de dados em qualquer lugar do mundo. À essa altura, fica claro que a nuvem não é um mecanismo físico, embora os servidores em que ficam armazenados os dados o sejam. O país com o maior número de servidores em seu território é a Irlanda, fato esse atribuído pelos impostos mais baixos e as terras mais baratas no período de instalação das

[11] Ramnath K. Chellappa é reitor associado e diretor acadêmico do programa de mestrado em análise de negócios da Emory University, sendo especialista nas áreas de mercados eletrônicos, preços, pirataria de produtos digitais e economia da segurança e privacidade da informação. Além disso, Chellappa é professor de sistemas de informação e gerenciamento de operações da Fundação Goizueta, vinculada a Goizueta Business School, pertencente à Emory University. O episódio mencionado trata sobre a pesquisa que concedeu a ele o seu PhD, visto que seu trabalho forneceu a primeira definição acadêmica do termo "*cloud computing*". Para mais informações, acesse: https://goizueta.emory.edu/faculty/profiles/ramnath-k-chellappa.

[12] A programação Lisp, nome advindo da expressão *List Processing*, foi concebida pelo cientista de computação John McCarthy em 1958. A motivação de McCarthy foi a ideia de desenvolver uma linguagem algébrica para processamento de listas, que seriam utilizadas em trabalhos de Inteligência Artificial (IA), de modo que a programação nasceu como uma ferramenta matemática. A denominação decorre do fato de que a lista é a estrutura de dados fundamental nesta linguagem, visto que tanto os dados quanto o programa são representados como listas, permitindo a manipulação do código fonte como qualquer outro tipo de dado. Veja mais em: https://ww2.inf.ufg.br/~eduardo/lp/alunos/lisp/intro.html.

empresas. Até pouco tempo, as *big techs*[13] instaladas na Irlanda[14] poderiam arcar com impostos pelo menos 11% mais baixos do que em outros países, como a Inglaterra, Alemanha e França. No entanto, com a proposta de imposto global mínimo de 15%[15], é possível que essa configuração seja alterada.

Sendo assim, fica claro que cada empresa pode optar pela instalação de servidores no local que lhe for mais favorável. No caso do Brasil, os arquivos dos usuários nativos ficam distribuídos em território nacional e estrangeiro, a depender da empresa, visto que o país ainda não apresenta um número de *data centers* suficiente para realizar todo o armazenamento no próprio país. Por exemplo, os arquivos de usuários brasileiros do Office 365, pacote de aplicativos em nuvem da Microsoft, ficam distribuídos entre EUA, Chile e Brasil. No entanto, deve-se diferenciar os serviços de armazenamento em nuvem e computação em nuvem, visto que são ferramentas distintas, embora ambas utilizem servidores para o armazenamento de dados.

O *cloud computing* permite que as empresas utilizem uma infraestrutura completa de computação, mediante pagamento, para a operação da companhia, enquanto o armazenamento em nuvem se limita ao arquivamento de informações. Em uma tentativa de tornar a situação mais clara, pode-se utilizar o Google como exemplo: o Google Cloud é o sistema de *cloud computing* da empresa, ao passo que o Google Drive é o sistema de armazenamento em nuvem da companhia. Sendo assim, é possível compreender que o *cloud computing* versa sobre um ambiente organizacional que abrange inúmeras possibilidades de atuação, como criação de soluções, uso de ferramentas on-line, codificação de aplicações de forma remota, entre outros, conforme será abordado posteriormente.

Em relação ao percentual de participação de *cloud computing* no Brasil, a sua aceitação em termos de gastos totais de TI está entre 8% e 9%, o que corresponde a cerca de metade da porcentagem dos Estados Unidos, conforme abordado pelo diretor sênior de pesquisa do Grupo

---

[13] As *big techs* são os principais provedores de serviços de nuvem estrangeiros, dominando a participação no mercado por meio de economias de escala e integração vertical, conforme definição da Aliança de Infraestrutura Digital Sustentável (SDIA). Em suma, tais empresas são as líderes no mercado de tecnologia da informação, de modo que as *big five* são a Alphabet (Google), Apple, Meta, Amazon e Microsoft. Para complementações, acesse: https://sdialliance.org/dictionary/big-tech/.

[14] Nesse ponto, pode-se mencionar a técnica do double irish with a dutch sandwich, esquema de elisão fiscal utilizado pelas big techs para reduzi sua responsabilidade fiscal. Para saber mais: https://www.investopedia.com/terms/d/double-irish-with-a-dutch-sandwich.asp.

[15] CNN Brasil Business. Entenda o que é o imposto mínimo global apoiado por líderes do G20. **CNN Brasil**, 2021. Disponível em: https://www.cnnbrasil.com.br/business/entenda-o-que-e-o-imposto-minimo-global-apoiado-por-lideres-do-g20/#:~:text=A%20taxa%20de%2015%25%20ser%C3%A1,%24%20845%20bilh%C3%B5es)%20por%20ano. Acesso em: 27 mar. 2023.

Gartner, Henrique Cecci, durante o AWS Summit no ano de 2022[16]. Contudo, o Brasil possui uma quantidade razoável de servidores e *data centers* de nuvem, sendo considerado um *hub* para a América Latina, os quais se encontram principalmente em grandes capitais, como São Paulo e Rio de Janeiro. Dessa forma, pode-se considerar que a adoção do *cloud computing* ainda é recente no Brasil, principalmente pelas dificuldades da sua implantação no país.

Nesse sentido, é importante pontuar que o Brasil apresenta alguns empecilhos na adesão às tecnologias que utilizam *data centers*, de modo geral. Tal fato ocorre, principalmente, pela questão da temperatura e dos sistemas de energia elétrica, visto que quanto mais quente for o clima do país em questão, maior o valor gasto com os processos de resfriamento de tais ferramentas. Nesse ponto, ainda pode-se mencionar a necessidade da transmissão de dados com baixo tempo de latência, o que não ocorre no Brasil. Sendo assim, por trás da nuvem, existem diversos componentes físicos que influenciam a sua aplicabilidade. No entanto, apesar das dificuldades mencionadas, é importante mencionar que existem serviços de cloud *computing* com servidores localizados em território nacional.

Além das empresas mais conhecidas no setor, como a AWS e a GCP, que possuem servidores no Brasil, pode-se mencionar outras, como a Hostinger, a Cloudways, o KingHost e o Locaweb. Essa última, inclusive, foi uma das primeiras empresas a trazer a hospedagem *cloud* para o Brasil, possuindo servidor no território nacional. Em sentido similar, a KingHost é uma empresa totalmente nacional, que possui um serviço adaptado ao público brasileiro, bem como é detentora de servidores em várias regiões do país. Uma empresa conhecida principalmente no território nacional é a UOL, a qual também desenvolveu seu sistema de computação em nuvem, o UOL Host.

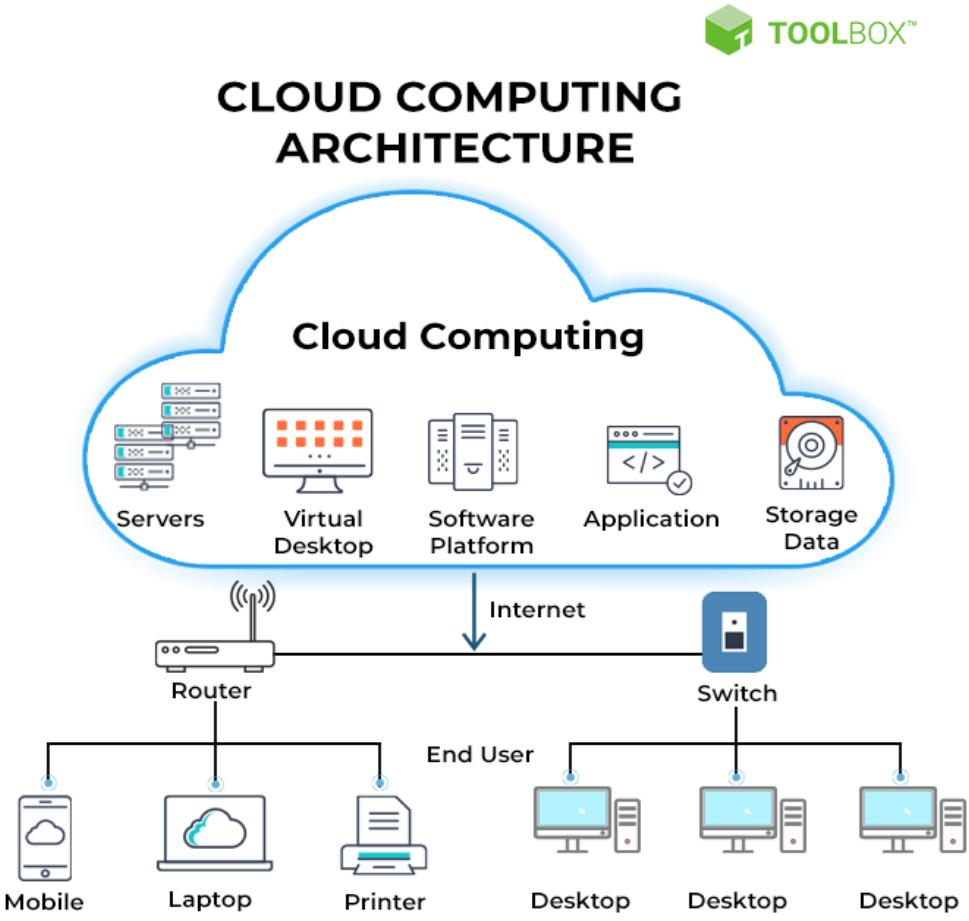
O UOL Host se destaca no território nacional não somente por possuir servidores no país, mas pelos preços atrativos, já que possuem planos a partir de R$ 22,90 por mês. Por conta da localização dos servidores, serviços personalizados e preços acessíveis, as empresas nacionais de *cloud computing* são uma excelente escolha. Cabe ressaltar que a localização do servidor atua diretamente na velocidade do sistema, visto que, quanto mais próximo o servidor, mais rápido os dados são transmitidos. Nesse sentido, as empresas de atuação global, como a AWS, GCP e Microsoft Azure podem ficar em segundo plano na escolha do sistema de nuvem.

[16] REDAÇÃO da Abranet. Brasil ainda é imaturo no uso de computação em nuvem. **Abranet**: Associação Brasileira de Internet, 2022. Disponível em: https://www.abranet.org.br/Noticias/Brasil-ainda-e-imaturo-no-uso-de-computacao-em-nuvem-3983.html?UserActiveTemplate=site&UserActiveTemplate=mobile#.Y9HqX3bMLrc. Acesso em: 27 mar. 2023.

No entanto, é importante pontuar que as empresas multinacionais utilizam o mesmo sistema de *cloud computing* em todas suas filiais, de modo que as empresas internacionais ganham vantagem nesse aspecto. Embora a Amazon Web Services ainda seja a líder mundial de computação em nuvem, o desempenho do Google Cloud Platform vem ganhando destaque, principalmente por agregar outras ferramentas da marca no produto, como o Google Ads. Por sua vez, o Microsoft Azure ainda é um sistema de pouca notoriedade no Brasil, embora possua pacotes completos e com ótimo custo-benefício.

De modo a tornar a compreensão do funcionamento da computação em nuvem mais claro, pode-se visualizar a imagem a seguir, que retrata a arquitetura dessa ferramenta:

Figura 1 - Arquitetura do *cloud computing*



Antes de prosseguir com o detalhamento da ferramenta, é importante diferenciar a arquitetura de nuvem e a infraestrutura de nuvem. A primeira se refere à forma como as tecnologias individuais são integradas visando a criação dos ambientes de *cloud computing*, isto é, o modo como todos os componentes de uma nuvem são conectados. A segunda é a ferramenta necessária para desenvolver uma nuvem, a qual se baseia na arquitetura como

referência. Desse modo, a infraestrutura é o conjunto dos elementos, enquanto a arquitetura é a organização de tais conjuntos.

Como visto na imagem, o *cloud computing* é formado por diversos componentes: os servidores, que são sistemas computacionais formados por hardware e software; o desktop, ferramenta utilizada pelos usuários[17]; a plataforma de software, que será vista posteriormente; a aplicação, que é o sistema pelo qual os usuários acessam os dados; e os dados armazenados, que são disponibilizados pelos titulares e tratados pelos usuários do sistema. No que se refere aos servidores, é importante mencionar que o hardware trata sobre os componentes palpáveis de um dispositivo eletrônico, enquanto o software é a parte lógica de tais componentes.

Nesse sentido, o hardware é a parte física que se encontra distribuída em diversas localizações geográficas, sendo composto por inúmeros equipamentos, como roteadores, matrizes de armazenamento, dispositivos de backup e servidores, por exemplo. A virtualização é o que conecta os servidores entre si, de modo a criar uma separação entre as funções e serviços de TI e o hardware. No hardware físico, instala-se um software chamado de hipervisor, que é o responsável por abstrair os recursos da máquina, como memória, potência de computação e armazenamento. A partir disso, geram-se recursos virtuais, os quais são alocados em aglomerados centralizados, denominados de *pools*.

Os *pools*, por sua vez, são as nuvens virtuais, as quais permitem o acesso de forma dinâmica e remota. A virtualização, como dito anteriormente, abstrai o espaço de armazenamento dos sistemas de hardware, possibilitando o acesso pelos usuários como armazenamento em nuvem. Com essa transformação, pode-se adicionar ou remover unidades, reaproveitando o hardware, além de responder às mudanças sem provisionar servidores individuais em cada nova iniciativa, diferenciando-se dos sistemas de data centers[18]. Por fim, outro elemento é a rede, como a Internet ou intranet[19], a qual possibilita o fornecimento dos recursos de nuvem aos usuários, mediante o acesso remoto sob demanda.

---

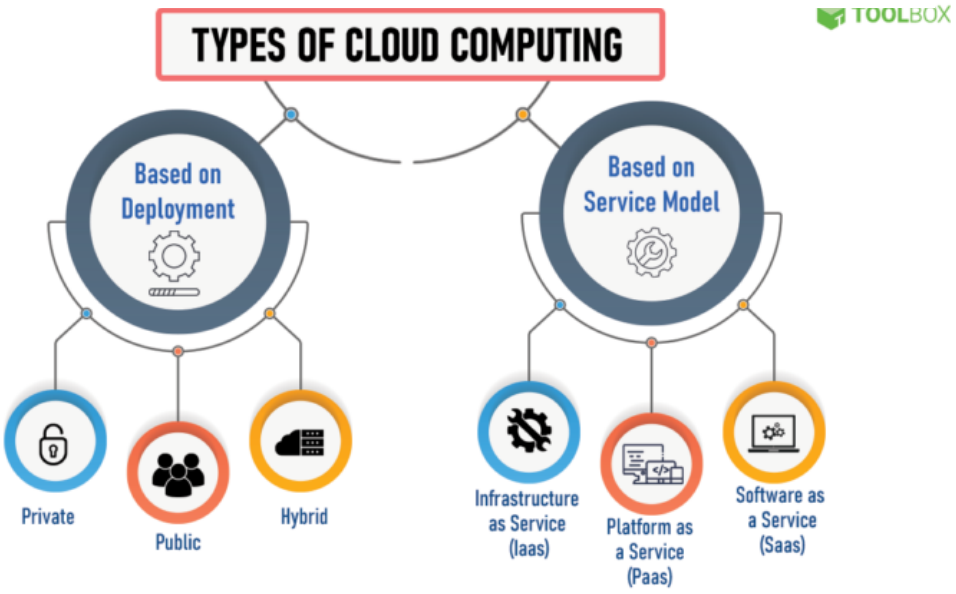
[17] O termo "usuários" é amplo e, embora a expressão em questão esteja retratando indivíduos de modo geral, deve ser entendido como "empresas privadas e órgãos públicos" no presente trabalho, visto que o *cloud computing* é um sistema de computação utilizado em situações de grande fluxo de informações, o que inclui aplicativos, sistemas e dados envolvidos nas operações.

[18] Um *data center* é uma instalação física de hospedagem de aplicativos e dados críticos, composta por uma rede de recursos de computação e armazenamento. Os principais componentes de um data center incluem alguns dos elementos vistos nas páginas anteriores, como roteadores, sistemas de armazenamento e servidores. No próximo subcapítulo serão vistas as diferenças entre a computação em nuvem e a utilização de *data centers*, também denominado de computação local.

[19] A intranet é um sistema criado nos mesmos moldes da Internet, mas de uso exclusivo de uma organização, de modo que somente os integrantes desse órgão detém acesso aos conteúdos disponibilizados. O uso da intranet é comum em universidades e órgãos públicos, como ocorre na Justiça Federal. No entanto, a intranet se utiliza da Internet para o seu funcionamento, de modo que a distinção entre os dois sistemas pode ser complexa.

Com o intuito de aprofundar o entendimento sobre o *cloud computing*, é importante compreender sobre os tipos de computação em nuvem, os quais serão melhor explicitados abaixo, mas podem ser resumidos conforme a imagem abaixo:

Figura 2 – Tipos de *cloud computing*



No que concerne a classificação do *cloud computing*, os serviços hospedados na nuvem podem ser divididos em três modelos quanto ao tipo de implantação específico: *infrastructure-as-a-service* (*IaaS*), *platform-as-a-service* (*PaaS*) e *software-as-a-service* (*SaaS*). No modelo *IaaS*, o usuário não necessita gerenciar a infraestrutura de nuvem, tendo controle sobre o armazenamento, sistemas operacionais e aplicativos implantados, de modo que um provedor de serviços é responsável pelo restante. A seu turno, o tipo *PaaS* é uma forma de *cloud computing* que não exige o gerenciamento de infraestrutura subjacente dos usuários, cedendo a eles o controle sobre os aplicativos implantados.

Por fim, a forma *SaaS*, também conhecida como *hosted software* (software hospedado) ou *on-demand software* (software sob demanda), permite que os usuários acessem os aplicativos localizados em uma rede de nuvem remota diretamente pela web ou por uma *Application Programming Interface* (API)[20], não sendo necessária a instalação de aplicativos

[20] O *Application Programming Interface* (API) é, como a própria tradução livre pontua, a interface de programação de aplicativos, aplicada mediante um conjunto de regras que permite a comunicação entre aplicativos diferentes. Sendo assim, uma API atua como uma camada intermediária de processamento de transferências de dados entre sistemas dentro das empresas. Um exemplo claro é o processamento de pagamento de terceiros, como ocorre com sites como PayPal. Para entender mais, acesse: https://www.ibm.com/topics/api.

em dispositivos locais. Tal formato permite que as empresas simplifiquem a manutenção e o suporte, visto que o provedor de serviços comanda todos os componentes do sistema, como o hardware, o middleware[21], o software aplicativo e a segurança.

Por sua vez, em relação ao modelo de implantação, a computação em nuvem pode ser classificada como nuvem pública, privada e híbrida. A nuvem privada, também conhecida por nuvem interna, empresarial ou corporativa, oferta seus serviços para uso exclusivo de uma única organização, de modo que não possa ser acessada por ninguém externo à entidade em questão. Essa forma de nuvem fornece um nível mais alto de segurança, embora apresente a desvantagem de que a própria organização é a responsável por todo o gerenciamento e manutenção dos data centers, o que pode ser oneroso.

A nuvem pública, por sua vez, se refere aos serviços oferecidos por provedores terceirizados por meio da internet. De modo contrário à nuvem privada, as nuvens públicas são responsabilidade dos provedores de serviços, o que proporciona economia às empresas no que concerne à compra, gerenciamento e manutenção da infraestrutura de rede. Por conta das barreiras de entrada reduzidas, o que proporciona um acesso mais célere à tecnologia pelas pequenas empresas, startups e profissionais independentes, previu-se um crescimento de 18,4% para a nuvem pública em 2021[22].

Por último, temos a nuvem híbrida, que é aquela que combina os recursos da nuvem pública e privada. Em suma, esse formato permite que as organizações dimensionem sua infraestrutura local, de modo a abarcar os benefícios de uma nuvem pública com uma segurança similar à nuvem privada. No ano de 2021, previa-se uma adoção maior da nuvem híbrida, juntamente com a multinuvem[23], visando garantir uma maior resiliência de TI, por meio da redução do tempo de inatividade, problema que afetou os maiores provedores do mundo em 2020 e 2021[24].

---

[21] O middleware é um software de comunicação entre aplicações, o qual permite conectar tecnologias, ferramentas e bancos de dados, integrando-os em um único sistema. Na década de 1980, o middleware ganhou popularidade por promover a integração entre novos programas e sistemas anteriores, excluindo a necessidade de reescrita do código. Veja mais em: https://aws.amazon.com/pt/what-is/middleware/#:~:text=O%20middleware%20%C3%A9%20um%20software,voc%C3%AA%20possa%20inovar%20mais%20rapidamente.

[22] PATIL, Prajakta; BASUMALLICK, Chiradeep. What is Cloud Computing? Definition, Benefits, Types, and Trends. **Spiceworks**, 2022. Disponível em: https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/. Acesso em: 27 mar. 2023.

[23] O termo "multinuvem" é utilizado para os casos em que várias nuvens fornecem suporte a um ou mais aplicativos, o que pode ser feito por nuvens públicas ou privadas, em um ambiente heterogêneo. Para mais informações, acesse: <https://www.dell.com/pt-br/dt/learn/cloud/what-is-multi-cloud.htm.>.

[24] PATIL, Prajakta; BASUMALLICK, Chiradeep. What is Cloud Computing? Definition, Benefits, Types, and Trends. **Spiceworks**, 2022. Disponível em: https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/. Acesso em: 27 mar. 2023.

Além dessas classificações, a nuvem pode ser dividida em duas camadas diferentes: *front-end*, que é a camada com a qual os usuários interagem; e *back-end*, que é a camada formada por software e hardware, isto é, os computadores, servidores, servidores centrais e bancos de dados. Portanto, a camada *front-end* é aquela que permite o acesso aos dados que foram armazenados na nuvem por meio de um software de *cloud computing*, enquanto a camada *back-end* é o principal componente da nuvem, sendo inteiramente responsável pelo armazenamento de informações com segurança.

A partir das informações mencionadas acima sobre o surgimento, arquitetura e infraestrutura do *cloud computing*, pode-se analisar o desenvolvimento dessa ferramenta, a qual vem sendo considerada uma tecnologia em constante adesão e crescimento: incluindo todos os tipos de nuvem e modelos de serviço, o mercado de computação em nuvem foi avaliado em US$ 321 bilhões em 2019, valor que pode atingir a marca de mais de US$ 1 trilhão até 2026[25]. Nesse contexto, o ano de 2021 foi um ano marcante para a computação em nuvem, visto o ritmo acelerado de adoção em resposta à pandemia de COVID-19.

Sendo assim, é notório que a computação em nuvem trouxe drásticas mudanças à tecnologia da informação. Nesse universo, a Amazon Web Services (AWS) ganhou participação de mercado rapidamente, de modo que especialistas previram a possibilidade de um monopólio. No entanto, desde os últimos trimestres de 2020, a Microsoft apresentou um crescimento acelerado, diminuindo a distância entre as duas *big techs*. Em 2021, as concorrentes disputaram alguns dos maiores contratos do setor, como o acordo JEDI[26] com o Pentágono dos EUA, por exemplo.

Por todo o exposto, concebe-se que o *cloud computing* é uma tecnologia revolucionária, apresentando inúmeras vantagens em seu uso, principalmente no que concerne o acesso às informações de qualquer lugar do mundo, o que é extremamente útil em um contexto globalizado. No entanto, embora os benefícios da ferramenta sejam claros, diversas

---

[25] GLOBAL Cloud Computing Market Size & Share Will Reach USD 1025.9 Billion by 2026: Facts & Factors. **GlobeNewswire**, 2021. Disponível em: https://www.globenewswire.com/news-release/2021/01/22/2162789/0/en/Global-Cloud-Computing-Market-Size-Share-Will-Reach-USD-1025-9-Billion-by-2026-Facts-Factors.html#:~:text=%E2%80%9CAccording%20to%20the%20research%20study,%25%20from%202019%20to%202027%E2%80%9D. Acesso em: 27 mar. 2023.

[26] O acordo JEDI, abreviação para *Joint Enterprise Defense Infrastructure*, foi um contrato que visava a adoção da computação em nuvem pelo Departamento de Defesa dos Estados Unidos, o qual foi avaliado em US$ 10 bilhões ao longo de dez anos. No entanto, após diversos protestos e atrasos, o Departamento de Defesa emitiu um novo contrato, denominado *Joint Warfighting Cloud Capability* (JWCC), o qual foi concedido à Amazon Web Services, Google, Microsoft e Oracle. Para mais informações, acesse https://www.nationaldefensemagazine.org/articles/2022/12/20/pentagon-cloud-computing-enterprise-finally-moves-forward.

problemáticas envolvem a sua aplicação, principalmente quando focamos nos dados pessoais, visto que a sua proteção pode se encontrar ameaçada com a utilização de sistemas complexos como os métodos de nuvem, conteúdo que será abordado no próximo subcapítulo.

2.2 A APLICABILIDADE DO *CLOUD COMPUTING*: AS VANTAGENS E DESVANTAGENS DA TECNOLOGIA

De acordo com uma pesquisa realizada pela *451 Research*, empresa global de pesquisa e consultoria, 90% das organizações já utilizam algum tipo de serviço de *cloud computing*[27]. Tal fato é atrelado às vantagens apresentadas por essa ferramenta, visto a economia de tempo e recursos comparados àqueles necessários para a configuração de uma infraestrutura física completa de tecnologia da informação (TI). Em 2009, a Agência Europeia de Segurança de Redes e Informações (ENISA) emitiu informativo sobre os benefícios, riscos e recomendações para a segurança da informação, pontuando que

> As economias de escala e a flexibilidade da nuvem são tanto amigas quanto inimigas do ponto de vista da segurança. As concentrações maciças de recursos e dados apresentam um alvo mais atraente para ataques, mas as defesas baseadas em nuvens podem ser mais robustas, escalonáveis e econômicas.[28] (tradução livre)

Portanto, é possível concluir que, ao mesmo tempo que o *cloud computing* possui suas vantagens, essas podem ser prejudiciais no que concerne à segurança dos dados envolvidos nas operações, sendo essa a principal problemática atinente à transferência e armazenamento dos dados pessoais. Nesse sentido, pode-se pontuar como vantagens, além da redução de custos de manutenção e infraestrutura própria, a escalabilidade do sistema em relação ao número de usuários e armazenamento necessário, bem como a flexibilidade e liberdade fornecida aos funcionários, o que propicia uma maior colaboração dos funcionários em projetos que se encontrem no sistema.

Além desses benefícios, deve-se ressaltar o benefício da continuidade dos negócios, visto que o retorno ao trabalho em casos de interrupção ou crise no sistema é facilitado em comparação a outros métodos, como por exemplo, no caso de data centers; bem como a

---

[27] NEW Statistics Show the Advance of Cloud Computing. **Eukhost**, 2020. Disponível em: https://www.eukhost.com/blog/webhosting/new-statistics-show-the-advance-of-cloud-computing/. Acesso em: 27 mar. 2023.

[28] O texto original dizia o seguinte: "*The cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective*". Para ler o informativo completo, acesse: https://www.enisa.europa.eu/media/news-items/cloud-computing-speech.

vantagem competitiva, já que a nuvem aborda vários aspectos do negócio, o que é tido como um benefício frente aos concorrentes que não se utilizam desse sistema, considerando que o tempo e os recursos investidos são menores. Nesse ponto, a empresa International Business Machines (IBM) defende, em artigo próprio[29], a utilização da computação em nuvem, principalmente como plataformas de inovação, objetivando o desenvolvimento de uma força de trabalho altamente qualificada e de alta tecnologia.

Todavia, a computação em nuvem também apresenta desafios, principalmente no que concerne à segurança associada à essa ferramenta. Como citado anteriormente, os provedores dos serviços de *cloud computing* garantem a utilização de rigorosos padrões de segurança, como também contam com certificações do setor, porém o risco ao armazenar dados em nuvem não tende à nulidade. Assim como diversas outras tecnologias existentes no mercado, a computação em nuvem possui seus pontos frágeis, como a necessidade de compromisso financeiro; os riscos envolvendo à proteção de dados, que abrangem não somente a perda de dados, mas a possibilidade de vazamento de tais informações; e a dependência de conexão com a internet, o que também contribui para um maior tempo de inatividade.

Contudo, visando analisar as vantagens e desvantagens do *cloud computing* como método relacionado à transferência internacional de dados, entende-se necessário estabelecer um comparativo com outra estrutura similar[30]. Para tanto, optou-se por comparar a computação em nuvem com a computação local, vez que as equipes corporativas de TI continuam analisando os riscos e benefícios das ferramentas físicas em relação às nuvens. Por trás da escolha entre uma das estruturas, existem diversos fatores a serem considerados, os quais se baseiam, principalmente, nas necessidades organizacionais da empresa em questão.

Nesse ponto, pode-se mencionar o sistema de VPN, que também é muito conhecido na atualidade, principalmente pelo seu uso no teletrabalho durante a pandemia. O *Virtual Private Networks* (VPN) é, como a própria tradução sugere, uma rede privada virtual. Esse modelo é muito utilizado pela sua segurança, visto que fornece acesso seguro à intranet da organização em questão, por meio de criptografia, a partir de um local remoto. Nas palavras de Douglas E.

---

[29] A International Business Machines (IBM) é uma empresa norte-americana referência em soluções tecnológicas para a indústria e o comércio. A trajetória da IBM iniciou no século XIX com o intuito de desenvolver máquinas elétricas para contagem de dados do censo de 1890 dos Estados Unidos. A empresa, que começou com o estatístico Herman Hollerit, desenvolve, fabrica e vende hardwares e softwares, o que inclui sistemas de inteligência artificial, deep learning e supercomputadores. Para visualizar a íntegra do artigo, acesse: http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf.

[30] KANADE, Vijay. Cloud vs. On-Premise Comparison: Key Differences and Similarities. Spiceworks, 2021. Disponível em: https://www.spiceworks.com/tech/cloud/articles/cloud-vs-on-premise-comparison-key-differences-and-similarities/. Acesso em: 27 mar. 2023.

Comer, "a tecnologia foi originalmente concebida para proporcionar uma interligação de baixo custo entre os vários locais geográficos de uma organização".

No entanto, o uso da VPN demanda uma estrutura física de TI, de modo que a aplicação pode ser alocada na computação local. Sendo assim, embora seja uma excelente ferramenta para as empresas que desejam atuar de forma remota, principalmente porque garante uma maior segurança no tráfego de dados, principalmente pelo uso de criptografia, a ferramenta não se apresenta como solução à computação local de modo geral, não se opondo à mesma, visto que a empresa deverá manter sua estrutura de TI para garantir o funcionamento correto do sistema.

Sendo assim, a principal diferença entre o sistema local e em nuvem diz respeito ao controle de recursos e gerenciamento de infraestrutura, visto que a computação no local hospeda seus aplicativos em hosts locais, como desktops e estações de trabalho. Nesse sentido, cabe pontuar que a nuvem é uma solução de aceitação global, a qual acompanha a transição que a indústria de TI propõe a cada ano. No entanto, essa aceitação ainda não é total, uma vez que muitas empresas ainda têm fortes preferências pelas soluções locais, também denominadas *on-premise*, bem como a existência de certas barreiras à aplicação de sistemas de *cloud computing* em certas localidades, como acontece no Brasil, tendo em conta as questões energética e climática, por exemplo, abordadas anteriormente.

O maior ponto de convergência dos sistemas é que ambos lidam com a infraestrutura computacional, a qual é tratada na rede, no caso do *cloud computing*; enquanto é gerida nas instalações da organização quando falamos da computação local. Nesse ponto, pode-se falar também sobre a aplicação conjunta de tais sistemas, visto que o modelo de infraestrutura local pode adotar a computação em nuvem como solução temporária ou adicional para a execução da sua carga de trabalho, visto que, nesse quesito, o *cloud computing* fornece serviços que a computação *on-premise* não oferta, como o espaço de memória ilimitado e o backup realizado em períodos determinados.

No que concerne às tecnologias aplicadas, ambas estruturas são desenvolvidas por uma combinação de ferramentas tecnológicas: sistema operacional, plataforma de gerenciamento e interfaces de programação de aplicativos (APIs). As configurações de computação, a seu turno, vêm se tornando cada vez mais complexas, de modo que a personalização dos sistemas operacionais, bem como a necessidade de aplicativos complementares se mostram cada vez mais necessárias. Embora a computação em nuvem permita uma maior flexibilidade nesse ponto, a virtualização das operações não se limita a essa forma operacional: muitas empresas optam por operar nuvens privadas internamente, mediante o uso da computação local, promovendo o gerenciamento da carga de trabalho com a virtualização.

Um ponto relevante para as empresas é a automação da infraestrutura de TI, o que permite que a área de informática foque nas questões mais prementes, agregando valor à organização. A automação pode ser adotada na computação local, bem como em diferentes ambientes da nuvem, colaborando com o aumento da eficácia da implantação das cargas de trabalho e a redução de custos. Apesar das semelhanças, as diferenças entre as ferramentas são o ponto decisivo para a escolha das empresas. Tal escolha se baseia nas necessidades e dos recursos que cada instituição busca com a implementação da computação. Nesse ponto, pode-se mencionar cinco critérios para a escolha das empresas: custo inicial, implantação de recursos, segurança de dados, controles de dados e problemas de conformidade.

Em relação ao custo inicial, a nuvem apresenta vantagens, fato que se mantém no longo prazo, visto que o ambiente de nuvem tem pouco ou nenhum custo inicial, já que a infraestrutura utilizada é de propriedade do provedor, o que se estende à equipe técnica de manutenção. Na computação em nuvem, o pagamento é realizado conforme o consumo, forma concebida como *pay as you go*, o que é benefício para qualquer empresa, visto que as despesas contínuas de manutenção de hardware e consumo de energia são reduzidas, da mesma forma que o consumo de espaço.

No que concerne a sua aplicabilidade em decorrência da espécie empresarial, a nuvem se mostrou econômica e de fácil uso para as pequenas empresas, oferecendo diversas integrações a um custo acessível, o que também pode se aplicar às empresas de grande porte, a depender da área de atuação e demanda tecnológica. A implantação de recursos, a seu turno, trata sobre a localização dos métodos. No caso da computação em local, os recursos são implantados internamente no servidor da empresa em um ambiente físico. Por outro lado, na computação em nuvem, a implantação dos dados ocorre em um servidor de terceiros, o que apresenta seus riscos, embora apresente uma vantagem: a transferência de responsabilidade pela segurança ao terceiro envolvido.

Uma das principais questões envolvidas na escolha entre os servidores se refere à segurança dos dados, uma vez que, como visto acima, na computação em nuvem há a transferência de dados a outros servidores. Por conta da segurança, muitas empresas optam pela computação no local, o que garante maior proteção aos dados extra confidenciais, bem como aos dados confidenciais, como dados bancários ou credenciais governamentais, os quais não podem ser compartilhados com terceiros. Nesse ponto, surge um debate importante que é o ceticismo em torno da segurança ofertada pelo *cloud computing*, visto que a perda de autoridade sobre os dados reduz a credibilidade do método, embora a nuvem tenha obtido diversos

certificados de segurança, além de os dados serem criptografados, de modo que apenas o provedor e o cliente tenham acesso às chaves.

O tema da segurança é o principal no que concerne ao presente trabalho, de modo que será tratado em relação à Lei Geral de Proteção de Dados (LGPD) no próximo capítulo. Nesse sentido, é importante mencionar que existem inúmeros indicativos de que as tecnologias de segurança evoluirão para se tornarem nativas da nuvem, uma vez que esse é um dos maiores impeditivos à adoção desse método, principalmente quando se analisam estudos sobre a situação[31]. Tal fato resulta em um interesse significativo em torno do *Secure Access Service Edge* (SASE)[32], que é uma estrutura de segurança que permite o acesso seguro ao *cloud computing*, abrangendo todo o cenário de TI em nuvens, data centers, SaaS e dispositivos de ponta.

Todavia, a aplicação de ferramentas de segurança, como a SASE, pode não ser suficiente. Sendo assim, é importante que a empresa reflita e, se necessário, promova as adequações necessárias a alguns pontos internos antes de aderir ao sistema de *cloud computing*. Dentre esses pontos, encontra-se a escolha de um bom provedor de nuvem, de modo que haja um equilíbrio entre o orçamento de TI e o melhor retorno possível, tendo em mente alguns critérios como robustez, segurança e performance. Nesse ponto, é importante ressaltar que muitos provedores, como a AWS, o GCP e o Microsoft Azure apresentam, além dos critérios mencionados, preços acessíveis.

O aprimoramento da governança corporativa como um todo, mas especialmente acerca dos ativos e processos da empresa, é outro ponto a ser revisitado. Visando a aplicação correta do sistema de *cloud* na empresa, a companhia deve rever suas políticas internas, principalmente em relação ao uso das ferramentas tecnológicas, bem como promover o monitoramento contínuo dos membros das equipes. Outro ponto a ser levantado é a realização de backups

---

[31] Um exemplo de pesquisa que corrobora a informação dada advém do International Data Corporation (IDC), empresa líder em inteligência de mercado, que conduziu um estudo sobre a violação de dados na nuvem durante 18 meses. Os resultados demonstraram que quase 80% das companhias pesquisadas sofreram com violações no período. Dentre as consequências que esse tipo de incursão pode causar, a ameaça à propriedade intelectual e a perda de reputação e confiança são as mais prejudiciais, visto que delas decorrem perdas financeiras consistentes, o que influencia diretamente no valor da marca. Para mais informações sobre a pesquisa, acesse: https://www.securitymagazine.com/articles/92533-nearly-80-of-companies-experienced-a-cloud-data-breach-in-past-18-months.

[32] O *Secure Acess Service Edge* (SASE) combina inúmeras funções de rede e segurança, que são normalmente fornecidas em soluções pontuais isoladas, entregando um serviço de nuvem integrado. Os componentes da SASE são o *Software-Defined Wide Area Network* (SD-WAN), que é um modelo de redes de longa distância, o qual permite a sobreposição na nuvem, fornecendo uma arquitetura *multicloud* contínua; a segurança da nuvem, baseada em um conjunto de tecnologias de nuvem para proteção de ameaças; e o acesso à rede *zero-trust*, o qual verifica as identidades dos usuários, confirmando a segurança do dispositivo antes de permitir acesso às aplicações.

automáticos, o que garante uma rápida recuperação das informações, visto que todos os sistemas são falíveis.

Ainda, pode-se mencionar a aplicação de criptografia, o que confere maior segurança e tranquilidade à empresa, visto que esse instrumento impossibilita a leitura de arquivos, em caso de interceptação. O controle de dados, que também é uma medida importante, se apresenta como ponto convergente à segurança de dados. Nos modelos *on-premise*, as empresas armazenam seus dados em um servidor local, possuindo total controle sobre eles. No entanto, esse fator pode não ser um benefício, visto que o cloud computing permite um controle de dados e acesso eficiente, embora seja realizado, em certos tipos de *cloud computing*, pelo próprio provedor.

Nesse sentido, o setor de atuação empresarial demonstra relevância, uma vez que empresas de setores altamente regulados, como os bancos, em sua maioria, optam por permanecer na forma física. Por outro lado, a computação em nuvem não é transparente quanto à propriedade dos dados, porque, como visto anteriormente, os dados são mantidos em servidores alheios. Assim sendo, o sistema em nuvem é adotado, prioritariamente, em negócios em que a privacidade não é uma prioridade. Contudo, esse fato não é capaz de reduzir a proteção envolvida na operação, visto que, a depender do tipo de *cloud computing* utilizado, os dados são controlados diretamente pela empresa, sem intervenção do provedor.

Os problemas de conformidade dependem dos regulamentos empresariais, de modo que, em alguns casos, as empresas são obrigadas a armazenar seus dados em servidores locais, visando o controle total sobre eles. Como se sabe, as empresas atuam de acordo com as políticas de conformidade do governo, que tem como principal objetivo a proteção dos cidadãos. Tais políticas abrangem a proteção de dados, os limites de compartilhamento desses dados e a autoria das informações, como ocorre com a LGPD e o Marco Civil da Internet no Brasil. As organizações que precisam aderir às regulamentações normalmente optam pelo modelo local.

Embora a computação em nuvem siga políticas de conformidade específicas, a sua natureza terceirizada, no que concerne aos servidores, é tida como uma violação às políticas de conformidade gerais. Por conta disso, as agências reguladoras tendem a não escolher as soluções em nuvem[33], fato que pode ser alterado com as inovações e integrações promovidas

[33] Nesse aspecto, cabe mencionar que, dentre as políticas e legislações consultadas para o presente trabalho, não há menção expressa ao sistema de *cloud computing*. No entanto, embora seja de conhecimento público a utilização de *data centers* privados para a administração pública, esse é um fato que se apresenta como passível de alteração, visto que muitos governos, como o dos Estados Unidos, que possui seu próprio serviço de computação em nuvem, tendem a revisar os seus sistemas de computação, em vista dos benefícios apresentados pelas soluções atuais.

pelo setor de tecnologia, como a SASE. Além dos parâmetros vistos, é possível mencionar outros, como a flexibilidade e escalabilidade de operações, o envolvimento técnico, a economia de energia, o aprimoramento da banda larga e a recuperação de desastres, os quais também são decisivos na escolha da ferramenta a ser utilizada.

A flexibilidade e a escalabilidade são as responsáveis por garantir que a experiência do usuário não seja comprometida, visto que os aplicativos seguem em evolução. Nesse ponto, o sistema em nuvem se mostra mais vantajoso, visto que os ambientes locais não permitem a flexibilidade desejada por conta dos servidores físicos, de modo que o dimensionamento se torna desafiador. Além disso, os servidores em nuvem propiciam uma economia de custos, uma vez que os servidores são conduzidos conforme a conveniência, ou seja, podem ter seu uso ampliado ou reduzido de acordo com a necessidade dos usuários.

O envolvimento técnico se refere aos profissionais responsáveis que devem ser mobilizados para a configuração e manutenção dos servidores. Nesse quesito, também se observa a presença do elemento econômico, uma vez que a proporção de funcionários executando essa função é proporcional aos custos, aumentando conforme a infraestrutura sob custódia da empresa. No *cloud computing*, existem tipos de implantação, conforme visto no capítulo anterior, em que o provedor de serviços gerencia toda a organização, de modo que o usuário não necessita aplicar conhecimentos técnicos para utilizar a plataforma, reduzindo a tecnicidade a ser aplicada pela própria empresa.

A economia de energia é um ponto que já foi abordado no capítulo anterior, mas merece atenção especial, visto que a questão energética envolve outras áreas, como a ambiental, que é tão cara e relevante no cenário mundial atual. Nesse ponto, é importante observar que os sistemas locais possuem um custo excepcionalmente elevado, enquanto o sistema em nuvem detém mecanismos que impedem a sobrecarga do sistema energético, o que ocorre, por exemplo, com gerenciamento do fluxo de ar das estruturas, tido como uma técnica avançada para a solução desse tipo de impasse.

A possibilidade de melhoria de banda larga também é um quesito decisivo na escolha da tecnologia a ser adotada, visto que tal ponto depende da ampliação de servidores, o que pode ser custoso quando tratamos sobre a computação local. No entanto, a nuvem apresenta um impasse nesse ponto: a organização terá apenas as opções disponibilizadas pelos provedores de serviços de nuvem, enquanto os sistemas locais permitem a adoção da opção de conexão que atenda melhor os requisitos da empresa. De toda forma, a computação em nuvem permite uma flexibilidade, visto que a atualização de determinado componente depende da alteração do plano de nuvem, o que é relativamente simples.

O último ponto a ser analisado neste comparativo é a recuperação de desastres, visto que apagões, falhas no sistema e *malwares*[34] são recorrentes em qualquer método tecnológico. A grande dúvida surge quando se pensa na restauração dos sistemas, uma vez que os danos à infraestrutura são proporcionais aos custos e desafios envolvidos. Nesse sentido, quando se utiliza da computação local, a recuperação pode ser mais lenta e dispendiosa do que quando tratamos do *cloud computing*. Além disso, a nuvem permite acesso instantâneo a recursos em caso de acidentes, possibilitando o backup e a restauração de software e dados.

Após o comparativo, é nítido que ambos modelos possuem seus prós e contras, de modo que as necessidades, as particularidades e os objetivos de cada empresa devem ser analisados no processo de escolha. Essencialmente, os sistemas se diferem pelo controle de recursos e pelo gerenciamento de infraestrutura, que são pontos diretamente relacionados com a segurança envolvida nas operações, sendo este o critério mais relevante no que se refere ao armazenamento e a transferência internacional de dados pessoais, objeto de estudo do presente trabalho. Como analisado anteriormente, em relação à segurança dos dados, a computação local se demonstra mais efetiva a depender da atividade realizada na empresa, visto que há um controle total das operações e dos servidores.

Por esse motivo, muitas empresas ainda optam pela computação *on-premise*, em uma tentativa de impedir o vazamento dos dados pessoais. No entanto, embora os níveis de segurança se demonstrem maiores na computação local, a perda de dados pode ocorrer em ambos os sistemas. Como visto anteriormente, as falhas no sistema podem ocasionar a supressão e a destruição de dados, de modo que a recuperação tende a ser mais rápida no sistema de *cloud computing*. Além disso, os provedores de serviços em nuvem cuidam da alocação e da manutenção do espaço físico para seus usuários, fornecendo medidas de segurança específicas para cada forma de computação em nuvem, o que torna as violações de dados menos prováveis.

Dessa forma, embora ainda haja muito receio em utilizar as novas tecnologias, como o *cloud computing*, a tendência é que cada vez mais as empresas adotem essa ferramenta, visto que, até mesmo a questão da segurança é relativa entre os dois sistemas analisados no presente trabalho. Tal fato é comprovado pelo relatório de risco e adoção de nuvem da McAfee[35], uma

---

[34] O termo "*malware*" é utilizado para qualquer software malicioso, que tenha como objetivo prejudicar ou explorar dispositivos, serviços ou redes. Tal nomenclatura deriva da expressão "*malicious software*", tendo como principal exemplo os vírus de computador. Para entender mais sobre o assunto, acesse: https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it.

[35] Cloud Adoption & Risk Report. **McAfee**, 2019. Disponível em: https://cts.businesswire.com/ct/CT?id=smartlink&url=https://www.skyhighnetworks.com/cloud-computing-trends-2019/&esheet=51890399&newsitemid=20181029005552&lan=en-US&anchor=Cloud+Adoption+&+Risk+Report+Landing+Page&index=2&md5. Acesso em: 02 jan. 2023.

das empresas de segurança digital mais renomadas do mundo, do ano de 2019, que concluiu que uma empresa média utiliza cerca de 1.935 serviços de nuvem. O número, que já era expressivo em 2019, segue aumentando, visto que o Brasil é o país da América Latina que mais utiliza plataformas e infraestruturas de nuvem, de acordo com o estudo "Como vamos na América Latina", realizado pela Citrix, empresa norte-americana de tecnologia[36].

Ademais, dentre as empresas pesquisadas, somente 27% delas não demonstraram interesse em aderir aos mecanismos de nuvem. Desse modo, o crescimento das ferramentas *cloud*, em especial o *cloud computing*, é uma tendência não somente no país, mas em todo mundo, sendo necessário abordar o tema de modo mais ostensivo, visando criar condições cada vez melhores para a aplicação dessas medidas, principalmente no que concerne a segurança dos dados envolvidos em operações de armazenamento e transferência. Nesse ponto, pode-se mencionar as próprias legislações atinentes à proteção de dados, visto que tais regulamentações fornecem parâmetros para as áreas de tecnologia da informação.

A Lei Geral de Proteção de Dados (LGPD), legislação de proteção de dados que fornece as diretrizes no país, em seu capítulo VII versa sobre a segurança e o sigilo dos dados, o que pode ser utilizado como diretriz no estabelecimento, aplicação e, até mesmo, na criação de sistemas tecnológicos. O art. 46 da LGPD é um exemplo de delimitação da proteção de dados pelos agentes de tratamento, impondo a adoção de medidas de segurança, técnicas e administrativas:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Sendo assim, a preservação dos dados pessoais é responsabilidade de cada agente de tratamento, definido como o controlador e o operador dos dados, de acordo com o art. 5º, IX, do mesmo diploma legal. No que concerne ao *cloud computing*, tanto as empresas contratantes do serviço como os provedores podem ser responsabilizados, de modo que ambas devem estar adequadas à LGPD, reduzindo assim as possibilidades de incidentes de dados. Cabe mencionar que, embora a probabilidade de ocorrência desses eventos possa ser reduzida, não há como certificar que algo assim jamais possa ocorrer, visto que os *malwares* são desenvolvidos em iguais termos e velocidade que as tecnologias preventivas e de reparação.

---

[36] A pesquisa está disponibilizada, em formato audiovisual, na plataforma YouTube, no seguinte link: https://www.youtube.com/watch?v=59Ug3u0PBYU.

Por conta disso, as empresas devem ter cuidados especiais com tais ferramentas, o que abrange a criptografia de dados, o controle de acessos, a autorização e autenticação de dados e usuários, conforme mencionado anteriormente. Em verdade, essas práticas podem ser adotadas mesmo quando da predileção pela computação local, visto que garantem uma maior segurança à empresa, o que também pode ser reforçado mediante a aplicação dos mecanismos de governança corporativa[37]. Sendo assim, as figuras referidas, juntamente com a compreensão e aprofundamento acerca da transferência e armazenamento internacional de dados pessoais, serão vistas no próximo capítulo, o qual objetiva responder a questão objeto de estudo do presente trabalho, utilizando-se dos conhecimentos obtidos neste capítulo sobre a tecnologia do *cloud computing*.

[37] De acordo com o Instituto Brasileiro de Governança Corporativa, a governança corporativa "é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas". Os princípios básicos da governança corporativa são a transparência, a equidade, a prestação de contas (*accountability*) e a responsabilidade corporativa. Como o *cloud computin*g é um mecanismo que visa melhorar a gestão das empresas, bem como permite um maior controle sobre os dados da empresa, envolvendo a segurança e a transparência de forma direta, pode-se entender o sistema como um aliado à governança. Para ler mais sobre a governança corporativa aplicada no Brasil, veja: <https://www.ibgc.org.br/conhecimento/governanca-corporativa>.

3 A TRANSFERÊNCIA E O ARMAZENAMENTO INTERNACIONAL DE DADOS PESSOAIS NACIONAIS

Até o momento, é possível concluir que, da mesma forma que a computação local, o *cloud computing* possui suas vantagens e desvantagens. No entanto, por ser um sistema que permite constantes atualizações, além de conceder o acesso remoto à uma complexa rede de operações e ferramentas, a computação em nuvem tende a ocupar cada vez mais espaço nas empresas, principalmente aquelas que optam pela adoção de ferramentas modernas, visando aprimorar os sistemas empresariais, bem como reduzir os custos operacionais. Nesse sentido, a questão da segurança é um problema que, com os avanços tecnológicos existentes, pode ser minimizado, como o *Secure Acess Service Edge* (SASE), visto no capítulo anterior, o que propiciaria a adoção da nuvem de forma ampla.

Em um país em que mais da metade da população relata que sofreu com vazamentos de dados ou conhece alguém que tenha passado por essa situação[38], não é difícil de entender que a ampla utilização da computação em nuvem ainda seja uma possibilidade relativamente remota. Nesse ponto, é importante relembrar que os ataques cibernéticos não ocorrem somente com indivíduos enquanto pessoas físicas, como frequentemente acompanhamos em episódios de hackeamento em redes sociais, mas com diversas empresas, o que resulta em consequências drásticas, de modo proporcional ao tamanho da companhia ou da quantidade de informações vazadas. Não é necessário pesquisar muito para encontrar diversos episódios de vazamento de dados, como o ocorrido no ano de 2021, que ficou conhecido como o maior vazamento de dados do Brasil[39].

Nesse evento, 223 milhões de CPFs, 40 milhões de CNPJs e 104 milhões de registros de veículos foram expostos. Desse total, mais de 22 mil empresas tiveram seus dados hackeados

[38] De acordo com pesquisa encomendada pelo International Business Machines (IBM) e conduzida pela The Harris Poll, empresa americana de análise e pesquisa de mercado, 6 em cada 10 brasileiros sofreram ou conhecem alguém que sofreu com vazamento de dados. O estudo global, realizado em 11 países, incluindo o Brasil, envolveu cerca de 11 mil pessoas, demonstrando resultados preocupantes em relação ao país. Nesse sentido, pode-se mencionar a consciência da população frente ao compartilhamento de dados pelas empresas, bem como a perda de controle pessoal sobre o uso que tais companhias promovem com esses dados, medida que chega a 81% dos entrevistados brasileiros. Para saber mais sobre a pesquisa, acesse: <https://www.ibm.com/blogs/ibm-comunica/estudo-da-ibm-aponta-que-96-dos-brasileiros-acreditam-que-as-empresas-nao-protegem-seus-dados-pessoaisestudo-da-ibm-aponta-que-96-dos-brasileiros-acreditam-que-as-empresas-nao-protegem-seus-dados-pess/>.

[39] MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 27 mar. 2023.

e divulgados livremente na internet, o que propiciou diversos golpes e fraudes[40]. Tais números espantam, visto que a quantidade de dados vazados é maior que a população brasileira, contabilizada em mais de 215 milhões de habitantes, de acordo com a projeção do IBGE[41]. No entanto, os ataques aos sistemas latino-americanos podem ser explicados por um fato determinante: a digitalização acelerada da América Latina. Beethovem Dias, engenheiro de soluções da F5 Brasil, empresa identificadora de ameaças cibernéticas, pontuou que

> Ambientes digitais foram se expandindo sem, no entanto, serem acompanhados das corretas políticas de segurança - isso faz da América Latina e do Brasil universos cada vez mais digitalizados, mas com pouca maturidade em segurança. Com isso, a superfície de ataque da região aumentou muito em 2020.

No entanto, de acordo com pesquisas realizadas em 2021 pela Surfshark[42], o Brasil é apenas o 6º país com o maior número de vazamentos de dados, ficando atrás de países como Estados Unidos, que ocupam o 1º lugar no ranking, seguidos de Irã e Índia. Ademais, segundo estudos da empresa de segurança Tenable[43], dos mais de 40,4 bilhões de vazamentos de dados que ocorreram no mundo em 2021, cerca de 815 milhões casos são brasileiros, registrando um aumento de 78% no total de registros. Em nível global, as grandes vítimas foram as empresas e instituições dos setores de saúde, juntamente com a área educacional e governamental.

Os dados são alarmantes, mas não surpreendem: a revista *The Economist*, em artigo publicado em 2017[44], previu o alcance dos dados pessoais. A revista considerou os dados pessoais como os ativos mais valiosos do mundo atual, sendo denominados, inclusive, de "novo petróleo". Por conta disso, chega-se à conclusão de que os dados se tornaram insumos de produção, de modo que, cada vez mais, esses componentes serão essenciais para a economia da sociedade da informação, também chamada de *data economy*. Nesse sentido, o artigo alerta para o fato de que o controle dos dados pelas companhias de Internet disponibiliza um poder enorme a elas.

---

[40] Conforme pesquisas feitas para o presente trabalho, a identificação da origem do vazamento, bem como a consequente responsabilização dos culpados ainda não ocorreu. Tal ponto demonstra uma possível fraqueza do sistema de proteção de dados nacional, visto que, em rápida consulta pelos noticiários digitais, é possível encontrar informações divergentes sobre a origem dos dados vazados e os responsáveis pelo ato. No entanto, como a aplicação das punições previstas na LGPD iniciaram somente em agosto de 2021, deve-se ter cautela ao analisar tais situações, uma vez que a questão ainda não é sedimentada no país.

[41] PROJEÇÃO da população do Brasil e das Unidades da Federação. **IBGE**: Instituto Brasileiro de Geografia e Estatística, 2023. Disponível em: https://www.ibge.gov.br/apps/populacao/projecao/. Acesso em: 27 mar. 2023.

[42] A pesquisa está disponível no seguinte link: https://surfshark.com/blog/data-breach-statistics-by-country.

[43] A pesquisa pode ser encontrada no link: https://www.tenable.com/press-releases/tenable-research-reveals-over-40-billion-records-were-exposed-in-2021.

[44] THE world's most valuable resource is no longer oil, but data. **The Economist**, Londres, 06 de maio de 2017. Disponível em: https://econ.st/3oeRM7G. Acesso em: 26 fev. 2022.

Logo, compreende-se que a segurança de dados é um aspecto essencial para a manutenção e armazenamento dessas informações, em especial no ambiente digital. No capítulo anterior, concluímos que, em questões de segurança, a computação local pode ser mais efetiva, visto que há um controle total dos dados pela própria empresa. Contudo, não é difícil entender que, quanto maior a empresa, maior o número de dados e, consequentemente, maior a equipe técnica que deve estar frente à proteção dessas informações. É nesse momento que o *cloud computing* se mostra uma potência: além de possuir uma maior capacidade de armazenamento, os dados hospedados no ambiente on-line são mantidos pelo provedor utilizado, o qual se compromete pela sua guarda e manutenção.

Por conta disso, as chances de ataques cibernéticos são reduzidas, já que os provedores, como Amazon e Google, contam com as melhores equipes técnicas, garantindo a segurança dos dados a todo momento. Ademais, em caso de ataque, a existência de backups propicia um retorno mais rápido às atividades empresariais, além da minimização de impactos, visto que os profissionais envolvidos nessa operação detêm conhecimentos avançados para tais atribuições. Como mencionado anteriormente, os fatores externos acarretam em risco aos dados mantidos em servidores locais, visto que quedas de energia e aquecimento excessivo das máquinas podem ocasionar em uma falha total da computação, o que resultaria na perda das informações, muitas vezes, em caráter irreversível.

No entanto, algumas controvérsias, como as questões energéticas e de disponibilidade de rede, já mencionadas no presente trabalho, dificultam a instalação de servidores de *cloud computing* em território nacional. Sendo assim, as empresas que adotam a computação em nuvem normalmente se relacionam com provedores internacionais, os quais mantêm seus servidores, em sua maioria, no estrangeiro. Além do exemplo do Office 365, citado no subcapítulo 1.1, pode-se mencionar, com o intuito de corroborar a informação anterior, os servidores do Google Cloud Platform (GCP), os quais se localizam, em especial, no continente norte-americano e europeu.

É nesse cenário, portanto, que a transferência internacional de dados se encontra no que tange o presente trabalho. Nesse sentido, cabe mencionar que o uso de sistemas de nuvem ocorre mediante a transferência constante de dados, tanto no que concerne o armazenamento em servidores internacionais como a própria transferência de dados realizada entre empresas e suas filiais localizadas no estrangeiro. No entanto, o conceito de transferência internacional de dados fornecido tanto pela LGPD quanto pelo GDPR não caracteriza de forma satisfatória a

operação[45]. Por esse motivo, o *European Data Protection Board* (EDPB) forneceu uma conceituação mais apurada, identificando três critérios cumulativos para qualificar a operação de transferência internacional de dados:

> 1) Um controlador ou um processador ("exportador") está sujeito ao GDPR para o processamento em questão.
> 2) O exportador divulga por transmissão ou de outra forma torna os dados pessoais, sujeitos a este processamento, disponível para outro controlador, controlador conjunto ou processador ("importador").
> 3) O importador está em um terceiro país, independentemente de este importador estar ou não sujeito ao GDPR para o processamento dado de acordo com o Artigo 3º, ou é uma organização internacional.[46] (tradução livre)

Sendo assim, visando aclarar a questão por meio de exemplos, apresenta-se a figura abaixo[47], que trata de algumas atividades que podem ser compreendidas como transferência internacional de dados:

[45] No entanto, da mesma forma que o EDPB promoveu essa explicação, entende-se que a ANDP irá abordar a questão quando da sua regulamentação. Nesse sentido, cabe pontuar que a tomada de subsídios da autoridade nacional sobre transferência internacional já sugere uma convergência à autoridade europeia.

[46] O texto original aponta o seguinte: " *1) A controller or a processor ("exporter") is subject to the GDPR for the given processing. 2) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer"). 3) The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.*". A informação pode ser encontrada em: https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf.

[47] FUNDAÇÃO GETULIO VARGAS. **Guia de Proteção de Dados Pessoais - Transferência Internacional**. Versão 1.0, Outubro, 2020, p. 13. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/transferencia_internacional.pdf . Acesso em: 23 fev. 2023

Figura 3 - Exemplos de atividades que configuram como transferência internacional

Exemplo	Descrição
Troca de e-mails	Imaginando que seja encaminhado e-mail de uma pessoa natural no Brasil para destinatário na Inglaterra. Caso esse e-mail contenha planilhas ou documentos com dados de candidatos a determinada vaga, alunos ou funcionários, esta operação caracteriza transferência internacional de dados.
Acesso a sistema no exterior	Uma executiva de determinada multinacional realiza viagem internacional e acessa em seu computador informações sobre clientes em seus arquivos e no sistema de sua empresa. Isso não caracteriza transferência internacional de dados. Contudo, se forem repassados dados a terceiros por meio desse sistema, se configura transferência.
Ligação telefônica	Um funcionário de determinada empresa estrangeira realiza uma ligação ao seu supervisor, passando dados sobre investimentos e ativos de dois de seus clientes, pessoas físicas brasileiras. Findada a ligação, o supervisor registra e armazena os dados em seu computador no sistema da empresa estrangeira. Está caracterizada a transferência internacional de dados.

Além disso, é necessário pontuar a origem das regulações acerca da transferência internacional de dados pessoais, de modo que o entendimento da Lei Geral de Proteção de Dados (LGPD), que é a legislação brasileira que abarca essa temática, se torne mais simplificado. Sendo assim, as legislações acerca da transferência internacional de dados iniciaram com uma política: as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais[48], também conhecido como Diretrizes sobre a Privacidade, publicada pela Organização para Cooperação e Desenvolvimento Econômicos (OCDE)[49] em 1980.

[48] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. **OECD**: Organisation for Economic Co-operation and Development, 2002. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 23 fev. 2023.

[49] A Organização para Cooperação e Desenvolvimento Econômicos (OCDE) é um grupo formado por diversos países dedicados, principalmente, ao desenvolvimento e cooperação econômicos, embora promovam o debate sobre outros temas, como questões sociais e políticas. Historicamente, o grupo foi formado pelos países europeus afetados pela 2ª Guerra Mundial.

No entanto, as Diretrizes sobre a Privacidade não detinham caráter cogente, de modo que, no ano seguinte, surgiu o primeiro instrumento internacional de natureza jurídica vinculativa: a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108) do Conselho da Europa[50]. Em outubro de 1995, o Parlamento Europeu, em conjunto com o Conselho da Europa, publicou a Diretiva 95/46/CE[51], conhecida por Diretiva de Proteção de Dados, versando sobre a proteção ao tratamento dos dados pessoais, bem como os critérios para a livre circulação desses dados.

A Diretiva foi revogada somente com a aprovação do *General Data Protection Regulation* (GDPR)[52] em 2016. Contudo, o GDPR entrou em vigor somente em 2018, mesmo período em que surgiu no mesmo ano em que foi editada a LGPD. Por ter sido a legislação precursora acerca da proteção de dados pessoais, o GDPR inspirou inúmeros outros regulamentos, como a própria legislação brasileira. Em seu art. 44[53], a regulação europeia prevê o princípio geral de transferências internacionais:

> Art. 44. Qualquer transferência de dados pessoais que estejam a ser tratados ou se destinem a ser tratados após a transferência para um país terceiro ou para uma organização internacional só pode ocorrer se, sem prejuízo das outras disposições do presente regulamento, forem cumpridas as condições previstas no presente capítulo pelo controlador e processador, inclusive para transferências posteriores de dados pessoais do país terceiro ou de uma organização internacional para outro país terceiro ou para outra organização internacional. Todas as disposições do presente capítulo devem ser aplicadas a fim de assegurar que o nível de proteção das pessoas singulares garantido pelo presente regulamento não seja comprometido. (tradução livre)

A partir disso, pode-se analisar a transferência internacional de dados na perspectiva da Lei Geral de Proteção de Dados (LGPD). No período anterior à promulgação da LGPD, a previsão acerca da proteção de dados pessoais ficava à cargo de normas setoriais esparsas, como

---

[50] UNIÃO EUROPEIA. **Convention 108 of the Council of Europe for the protection of individuals with regard to the processing of personal data**. Disponível em https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf. Acesso em 23 fev. 2023.

[51] UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. [1995]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Acesso em: 23 fev. 2023.

[52] GENERAL Data Protection Regulation (GDPR). **GDPR.EU**, [202?] Disponível em: https://gdpr.eu/tag/gdpr/. Acesso em: 23 mar. 2023.

[53] O artigo original traz a seguinte previsão: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*". Disponível em: https://gdpr.eu/article-44-transfer-of-personal-data/.

o Marco Civil da Internet, bem como interpretações de outros códigos e da própria Constituição Federal (CF). Em relação à Constituição, pode-se mencionar os incisos IX (liberdade de expressão), X (inviolabilidade da vida privada e da intimidade), XII (inviolabilidade do sigilo de dados) e XIV (direito de acesso à informação) do art. 5º, os quais abarcam a proteção de diversos âmbitos dos dados pessoais.

Por sua vez, o Código Civil (CC) prevê, em seus arts. 20 e 21, a possibilidade de proteção das informações privadas como direito da personalidade, o que pode ser associado à proteção de dados. O Código de Defesa do Consumidor (CDC), que será mencionado em momento posterior, trata sobre a proteção dos dados pessoais utilizados em bancos de dados e cadastros de consumidores em seus arts. 43 e 44. No entanto, o primeiro diploma legal a tratar sobre os direitos dos titulares de dados pessoais, inclusive no que concerne à transferência internacional de dados, foi o Marco Civil da Internet, a Lei nº. 12.965/2014. Embora tenha sido a legislação pioneira sobre a temática, o Marco Civil da Internet não estruturou, de forma concisa, a transferência internacional de dados, o que veio a ser realizado somente com a LGPD.

No entanto, no que concerne o Marco Civil da Internet, merecem destaque dois artigos em especial: o art. 3º, inciso III, que versa sobre a proteção dos dados pessoais como um princípio do uso da Internet, e o art. 11, caput e parágrafos seguintes, os quais tratam sobre a aplicação da legislação brasileira em qualquer operação de coleta, armazenamento, guarda e tratamento de dados, desde que, pelo menos, um desses atos tenha ocorrido em território nacional.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> III - proteção dos dados pessoais, na forma da lei;
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Nesse sentido, é importante dizer que a regulamentação acerca da proteção de dados pessoais é específica em cada país, como ocorre com os Estados Unidos, o Chile e o Uruguai, que se diferem da proteção concedida no Brasil e na União Europeia. Sendo assim, os países possuem critérios diferenciados para autorizar a transferência internacional de dados, visto que os próprios modelos se diferem: o modelo geográfico é adotado pela União Europeia e Brasil, enquanto o modelo de responsabilização é adotado, por exemplo, pelo Canadá. No entanto, no caso do Brasil, o legislador se ocupou em garantir que o fluxo transfronteiriço de dados ocorra entre países que garantam a segurança nos moldes da legislação nacional, seguindo o exemplo do seu modelo inspirador. Tal fato é de extrema relevância, porque há uma garantia maior aos brasileiros quanto à salvaguarda dos seus dados.

3.1 ENQUADRAMENTOS LEGAIS ATINENTES À TRANSFERÊNCIA E ARMAZENAMENTO INTERNACIONAL DE DADOS PESSOAIS NACIONAIS

Quando pensamos sobre os enquadramentos legais atinentes à transferência e armazenamento internacional de dados, não é incomum que o primeiro pensamento seja a Lei Geral de Proteção de Dados (LGPD). No entanto, a proteção dos dados pessoais não se limita somente a esse diploma legal. Nesse sentido, deve-se pontuar que a proteção dos dados pessoais é uma garantia constitucional, visto que a Emenda Constitucional 115/2022 atribuiu caráter de direito fundamental a essas informações, passando a integrar o art. 5º da Constituição Federal.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Além da previsão do art. 5º da CF, a proteção de dados pessoais se encontra no art. 21, que prevê a competência da União para "organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei". O art. 22 da CF prevê, inclusive, a competência exclusiva da União para legislar sobre a temática. Nesse sentido, pode-se dizer que a Autoridade Nacional de Proteção de Dados (ANPD), que adquiriu o status de autarquia federal em outubro do ano passado, em decorrência da aprovação da Medida Provisória 1.124/2022, é responsável pela fiscalização e organização da proteção e tratamento de dados. A definição de autoridade nacional está disposta no inciso XIX do art. 5º da LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A ANPD nasceu vinculada à presidência da República, mas a alteração para autarquia especial é objeto de discussão desde 2019. A partir da modificação, a autoridade nacional garante sua autonomia administrativa e financeira. Segundo o Poder Executivo[54], o objetivo da mudança é evitar a descontinuidade administrativa da ANPD, bem como agregar maior confiabilidade ao sistema regulatório de proteção de dados. No novo formato, entende-se que a autoridade nacional encontrará compatibilidade com outros regimes regulatórios e experiências internacionais.

No que concerne à ANPD, deve-se pontuar que a situação da autoridade ficou pendente por alguns anos, gerando dúvidas sobre a criação da autoridade. Contudo, com a publicação da Medida Provisória nº. 869/2018, a concepção da autoridade foi devidamente incluída na legislação. A partir disso, a estruturação da ANPD foi iniciada, embora ainda haja questões pendentes, previstas nas agendas bienais, conforme será visto a seguir. Ademais, a LGPD prevê inúmeras atribuições à autoridade nacional, reservando um capítulo inteiro à ANPD, o capítulo IX da legislação nacional, em especial a seção I.

A LGPD é o instrumento legal que, de acordo com o seu art. 1º, dispõe sobre o tratamento de dados pessoais em território nacional, incluindo aqueles vinculados por meio digital. O diploma legal em questão é inspirado, conforme mencionado anteriormente, na *General Data Protection Regulation* (GDPR), de modo que muitos dispositivos da segunda possuem sua correspondência na legislação brasileira. Tal ocorre com a transferência internacional de dados, a qual está prevista no capítulo V de ambos regulamentos. No entanto, a definição de transferência internacional de dados está prevista no inciso XV do art. 5º da LGPD.

Nesse sentido, a transferência internacional de dados é "a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro". Por sua vez, a definição de dados pessoais também se encontra no mesmo artigo, no inciso I, apontando que dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável". Embora a transferência internacional de dados esteja, efetivamente, prevista nos arts. 33 a 36 da Lei em voga, o próprio art. 3º menciona a questão da localização dos dados, dispondo a

[54] AGÊNCIA Senado. Autoridade Nacional de Proteção de Dados é transformada em autarquia. **Senadonotícias**, 2022. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/10/18/autoridade-nacional-de-protecao-de-dados-e-transformada-em-autarquia. Acesso em: 27 mar. 2023.

aplicação da LGPD a "qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados"[55].

De toda forma, deve-se levar em consideração que todas as atividades de tratamento de dados pessoais devem, além de observar a boa-fé, cumprir os requisitos presentes nos incisos do art. 6º da LGPD. Os requisitos são, em verdade, os princípios que regem a proteção de dados, sendo eles a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e a responsabilização e prestação de contas. Tais princípios serão analisados de forma mais aprofundada a seguir. Por sua vez, as hipóteses em que a transferência internacional de dados pode ocorrer se encontram previstas no art. 33 da LGPD, que é o artigo central acerca da temática:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos;
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V - quando a autoridade nacional autorizar a transferência;
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

[55] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Inspirada na legislação europeia, a LGPD se desenvolveu a partir do juízo de adequação, em relação à circulação transfronteiriça dos dados pessoais. Sendo assim, tanto os dados pessoais de europeus, quanto os dos brasileiros, somente podem ser enviados para países que possuam um nível adequado aos padrões estipulados em legislação própria. Nesse cenário, a Autoridade Nacional de Proteção de Dados (ANPD) se mostra essencial: a sua atuação independente e a regulamentação de tais transferências, conforme previsão nos arts. 33 a 36 do mesmo diploma legal, favorece a inserção do país na globalização informacional[56].

Nas palavras de Tarcísio Teixeira e Ruth Guerreiro, "a eficácia de uma lei altamente rigorosa no que tange à proteção de dados pessoais depende da tutela específica da sua transferência para ordenamentos jurídicos estrangeiros"[57]. Portanto, a regulação da transferência internacional de dados se mostra tão importante, principalmente porque os dados podem ser facilmente transferidos pelos meios digitais, como ocorre, por exemplo, com o sistema de *cloud computing*, em que os dados são disponibilizados em servidores estrangeiros. Ademais, é importante pontuar que, embora hajam diversas hipóteses para a transferência internacional de dados, não há hierarquia entre elas, conforme mencionado por Marcel Leonardi:

> Vale ressaltar que não existe relação hierárquica entre os mecanismos de transferência. Aquele escolhido dependerá da finalidade e do contexto da transferência e da natureza dos dados pessoais, sendo necessário avaliar cuidadosamente cada caso concreto para se definir qual o mecanismo de transferência mais apropriado.[58]

A partir disso, pode-se analisar cada um dos incisos do art. 33 da LGPD, os quais preveem os mecanismos de transferência possíveis. O primeiro instrumento mencionado é o

---

[56] LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados.** (Coleção teses de doutoramento). São Paulo: Grupo Almedina (Portugal), 2020. *E-book*. ISBN 9788584936397. Pg. 11. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 19 dez. 2022.

[57] TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Comentada Artigo por Artigo. São Paulo: Editora Saraiva, 2022. *E-book*. ISBN 9786555599015. Pg. 38. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 14 jan. 2023.

[58] LEONARDI, Marcel. Transferência Internacional de Dados Pessoais. *In*: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. *E-book*. ISBN 9788530992200. Pg. 303. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 23 dez. 2023.

nível de proteção de dados pessoais do país ou organismo internacional que receberá os dados em questão. A análise da proteção é feita pela ANPD, conforme as previsões do art. 34 da lei em voga, a qual leva em consideração i) as normas gerais e setoriais em vigor no país ou organismo internacional; ii) a natureza dos dados; iii) a observância de princípios gerais de proteção de dados e direitos dos titulares; iv) a adoção de medidas de segurança; v) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados; e vi) outras circunstâncias específicas que forem relevantes para a transferência.

Nos casos em que o nível de proteção do país estrangeiro não é considerado adequado pela ANPD, pode-se utilizar outros critérios para a transferência, como as a) cláusulas contratuais específicas para determinada transferência; as b) cláusulas-padrão contratuais; as c) normas corporativas globais; os d) selos, certificados e códigos de conduta regularmente emitidos. No caso das cláusulas contratuais específicas, a transferência poderá ser realizada desde que tais cláusulas sejam devidamente verificadas e aprovadas pela Autoridade, de modo que, caso haja qualquer alteração em referidas cláusulas, a ANPD deve ser comunicada, realizando eventual reavaliação.

As cláusulas-padrão contratuais (CPC) são cláusulas-modelo que deverão ser criadas pela ANPD, as quais contêm as obrigações das partes envolvidas na transferência e os direitos dos titulares dos dados a serem transferidos. Quando há a adoção de tais cláusulas, o controlador pode realizar a transferência sem a anuência da ANPD ou dos respectivos titulares, visto que se trata do cumprimento de medidas previamente autorizadas pela Autoridade. No entanto, a LGPD é escassa em maiores orientações sobre as cláusulas-padrão contratuais, de modo que se acredita em uma nova influência da GDPR sobre a legislação nacional.

Nesse sentido, o direito europeu prevê as chamadas *Standard Contractual Clauses* (SCCs), as quais são divulgadas de forma on-line pela Comissão Europeia[59]. No que concerne o Reino Unido, o qual se retirou da União Europeia, o uso das SCCs é orientado, de forma integral e sem alterações, pelo *Information Commissioner's Office* (ICO), que é a autoridade responsável pela proteção de dados. Ademais, o ICO entende que é possível abranger outras cláusulas comerciais, contanto que não haja conflito com as SCCs. Ademais, cabe ressaltar que, embora se utilize o termo "cláusulas", as SCCs podem ser incorporadas como um capítulo dos contratos ou como um Anexo ao contrato principal.

---

[59] COMISSÃO EUROPEIA**. Cláusulas contratuais padrão para transferências internacionais**. União Europeia, 2021. Disponível em: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en. Acesso em: 20 fev. 2023.

Além das opções vistas acima, pode-se utilizar as normas corporativas globais, que são similares às *Binding Corporate Rules* (BCRs) do direito europeu. Tais normas se aplicam à transferência internacional de dados pessoais entre empresas do mesmo Grupo Econômico. O direito nacional é omisso a respeito, de modo que se espera que a ANPD adote um modelo similar às BCRs da GDPR. Nesse modelo, uma das empresas do Grupo submete a sua política interna de proteção de dados para avaliação da autoridade nacional competente, a depender da localização da empresa. De modo geral, tais normas corporativas abordam os princípios de proteção de dados pessoais, que, no direito brasileiro, se encontram no art. 2º da LGPD.

Contudo, as BCRs não se limitam às transferências internacionais, abordando os principais procedimentos e políticas internas, bem como outras medidas administrativas e organizacionais, além das técnicas adotadas por todo o grupo econômico na proteção de dados pessoais. A partir da autorização das BCRs, todas as transferências internacionais de dados intragrupo são permitidas, visto que as normas estão em conformidade com o GDPR. Da mesma forma que as cláusulas-padrão, caso haja alteração nas normas corporativas, deve-se comunicar à autoridade nacional para reanálise, conforme a disposição do art. 36 da LGPD.

A última hipótese do inciso II do art. 33 da LGPD trata sobre os selos, certificados e códigos de conduta, que permitem a transferência internacional quando reconhecidos pela ANPD. No entanto, tais certificações dependem da adoção da Autoridade nacional para o seu real funcionamento, de modo que o processo de reconhecimento desses mecanismos deverá, de acordo com o art. 35, § 1º, da lei em questão, considerar os requisitos, as condições e as garantias mínimas para a observância de direitos, garantias e princípios da LGPD. Nesse sentido, a ANPD pode, em conformidade com a LGPD, indicar organismos de certificação para validar os documentos, os quais podem ser revistos e, se necessário, anulados pela Autoridade, quando ensejar desconformidade com a lei.

O inciso III do mesmo artigo trata sobre a "necessária cooperação jurídica internacional", a qual abrange os órgãos públicos de inteligência, de investigação e de persecução, conforme os instrumentos de direito internacional. Tal hipótese é restrita, uma vez que o interesse público sobressai em relação aos direitos dos titulares dos dados pessoais, de modo que não haja aplicação direta para o setor privado. O inciso IV, por sua vez, trata da hipótese de transferência internacional em caso de necessidade para proteção da vida ou da incolumidade física, tanto de titular quanto de terceiro. Nas palavras de Marcel Leonardi, "seria,

inclusive, um contrassenso colocar em risco a vida ou a integridade física de alguém em nome da proteção de dados pessoais”[60].

A hipótese do inciso V é a mais genérica, dispondo que a transferência internacional pode acontecer “quando a autoridade nacional autorizar a transferência”. Levando em consideração a omissão da Lei quanto aos procedimentos envolvidos, bem como os critérios para autorização, entende-se que a ANPD deverá criar as normas e diretrizes para possibilitar a aplicação dessa competência. O inciso VI, de modo diverso, é específico, visto que aborda as transferências internacionais oriundas de compromissos assumidos em acordos de cooperação internacional.

A execução de política pública, prevista no inciso VII, é uma hipótese disponível apenas para a Administração Pública, de modo que a LGPD autoriza a transferência internacional de dados quando esta for necessária para a execução de política pública ou atribuição legal do serviço público. No entanto, para que isso ocorra, deve-se publicizar tais atos, conforme os termos do art. 23, I, do mesmo diploma legal.

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

No inciso VIII, encontra-se a hipótese do consentimento do titular dos dados pessoais que, conforme o art. 5º, inciso V, é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”. No inciso XII do mesmo artigo, tem-se a definição de consentimento, que é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. Portanto, entende-se que o consentimento deve ser obtido de forma específica para o fim que lhe será atribuído, ou seja, o titular deve ter ciência de que se trata de operação internacional, conforme entendimento do inciso mencionado.

Ademais, o consentimento deve ocorrer por escrito ou por outro meio que demonstre a manifestação de vontade do titular, conforme se depreende do caput do art. 8º da LGPD. Nesse

---

[60] LEONARDI, Marcel. Transferência Internacional de Dados Pessoais. *In*: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200. Pg. 305. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 23 dez. 2023.

sentido, cabe mencionar que são necessários "dois consentimentos": um para o tratamento dos dados e outro para a transferência, visto que se trata de duas bases legais a serem preenchidas. Desse modo, o controlador, que é aquele que possui o ônus da prova no que tange a Lei em análise, deve comprovar que obteve o consentimento do titular. Nesse quesito, cabe mencionar que a figura do controlador, conforme definido no art. 5º, inciso VI, é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Sendo assim, da mesma forma que o titular pode conceder o consentimento, ele pode retirá-lo, conforme previsão do art. 8º, § 5º, da mesma Lei.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Pelo que se depreende do parágrafo 5º, a revogação do consentimento não afeta as operações realizadas anteriormente, até que haja expresso requerimento de eliminação. Por tais razões, o uso do consentimento como mecanismo de transferência internacional não é recomendado, visto que, em caso de revogação do consentimento, compromete-se a continuidade das atividades de tratamento, bem como se dificulta o novo preenchimento dos múltiplos requisitos legais. Nesse sentido, pode-se pontuar que "o consentimento para transferências internacionais representa uma hipótese muito mais teórica do que prática, notadamente para o setor privado"[61].

O rol de hipóteses de transferência internacional encerra com a referência de três bases legais disponíveis para o tratamento de dados pessoais, previstas nos incisos II, V e VI, do art. 7º, da LGPD.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

[61] BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200. Pg. 307. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 23 dez. 2023.

Nos casos em que há o cumprimento de uma obrigação legal ou regulatória pelo controlador, conforme o inciso II, não se exige o enquadramento da atividade específica na legislação Nesse ponto, também importa mencionar que a LGPD não especifica a necessidade de a obrigação ser exclusivamente brasileira, de modo que a ANPD deverá emitir opinião sobre essa questão. De modo similar, a previsão do inciso V permite a transferência internacional de dados nos casos em que haja a execução de um contrato ou de seus procedimentos preliminares.

Em relação à hipótese do inciso V do art. 7º, o titular dos dados deve ser parte do contrato ou titular do pedido de execução dos procedimentos preliminares para que a transferência possa ser efetuada. Nesse caso, cabe a menção de que o termo "contrato" deve ser entendido de forma mais ampla, no que concerne à LGPD, visto que abarca todo tipo de acordo e relação jurídica de natureza contratual existente entre as partes, desde que observem os requisitos mínimos legais. A última hipótese legal para a transferência internacional de dados é o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Nessas situações, caso o controlador seja parte em um desses procedimentos, tanto no Brasil quanto no exterior, é possível utilizar a transferência internacional. É importante pontuar que o exercício regular de direitos abarca não somente os direitos do controlador, mas do próprio titular ou de terceiros que estejam envolvidos nas operações. Tal previsão é uma forma do legislador de facilitar o exercício do direito de defesa, de modo que não haja impedimentos legais para a transferência, viabilizando a solução célere e uma defesa mais acurada em casos internacionais.

O art. 34 da LGPD trata sobre os critérios de avaliação do nível de proteção de dados do país estrangeiro ou do organismo internacional que a ANPD deve utilizar, conforme mencionado anteriormente. Sendo assim, a equivalência entre as legislações será analisada pela autoridade nacional, de modo que, caso não preencham os requisitos, a transferência ainda possa ser realizada, desde que mediante a adoção de outros mecanismos, como as cláusulas contratuais-padrão e as normas corporativas globais, por exemplo. O art. 35 do mesmo diploma legal aprofunda a questão das hipóteses diversas:

> Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.
> § 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.
> § 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às

> operações de tratamento, quando necessário.
> § 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.
> § 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
> § 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

A adoção de modelos de cláusulas contratuais demonstra que as novas regulamentações buscam assegurar os preceitos legais e os princípios, direitos, garantias e deveres trazidos pela lei, de modo que sejam observados e pactuados em toda a cadeia de valor do negócio. Essa tática normativa tende a criar um caráter vinculante às cláusulas estipuladas a partir da própria legislação. Tal padronização se demonstra como uma estratégia, a qual pode ser observada na redação de órgãos regulatórios, como a Resolução nº. 4.658/2018 do Banco Central[62], que versa sobre a contratação de serviços na nuvem, trazendo artigos específicos sobre as cláusulas contratuais obrigatórias e vinculantes.

A transferência internacional de dados estava prevista no item 9 da agenda regulatória bianual 2021-2022 da ANPD, a qual foi aprovada pela Portaria nº. 11, de 27 de janeiro de 2021.

---

[62] Resolução Bacen 4.658/2018: "Art. 17. Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever: I – a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; II – a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I; III – a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes; IV – a obrigatoriedade, em caso de extinção do contrato, de: *a*) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição contratante; e *b*) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea *a* e a confirmação da integridade e da disponibilidade dos dados recebidos; V – o acesso da instituição contratante a: *a*) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III; *b*) informações relativas às certificações e aos relatórios de auditoria especializada, citados no art. 12, inciso II, alíneas *d* e *e*; e *c*) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados, citados no art. 12, inciso II, alínea *f* ; VI – a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição; VII – a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações; VIII – a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e IX – a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor. Parágrafo único. O contrato mencionado no *caput* deve prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil: I – a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do *caput*, que estejam em poder da empresa contratada; e II – a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que: *a*) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e *b*) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante".

Quando da análise acerca da temática, conclui-se que "as cláusulas-padrão contratuais têm sido o mecanismo de transferência internacional dados mais utilizado mundialmente, funcionando inclusive como ferramenta de convergência entre diferentes sistemas"[63]. Por esse motivo, as CPCs foram eleitas como o primeiro mecanismo a ser normatizado pela ANPD, sendo tido, inclusive, como a melhor opção para as pequenas e médias empresas.

É relevante mencionar que as CPCs são uma ferramenta que permite compatibilizar as regras de proteção de dados de jurisdições diversas, por meio de instrumento contratual, sendo, além disso, o mecanismo que apresenta o menor custo de implementação. Nesse sentido, as outras opções de mecanismos de transferência internacional de dados não apresentam o mesmo dinamismo para atender a necessidade urgente de regularizar tais instrumentos: as decisões de adequação constituem processos de análise morosos, além de atender apenas às localidades analisadas; os selos e certificações ainda não foram regulamentados pela ANPD, sendo um tema bastante complexo; e, por fim, os códigos de conduta possuem um espectro estreito de utilização.

Sendo assim, dada a urgência da regulamentação, a ANPD entendeu que iniciar pelas CPCs é a opção mais viável, visto que disponibiliza o mecanismo de maior alcance à população. Além disso, a regulamentação das cláusulas contratuais específicas e das normas corporativas globais segue critérios essencialmente similares, de modo que a autoridade reguladora optou por desenvolver, de modo inicial, a regulamentação desses três instrumentos de transferência internacional de dados, os quais foram denominados como "instrumentos contratuais".

Desse modo, nota-se que o Brasil ainda não reconheceu nenhum país como adequado para a transferência internacional de dados, visto que a ANPD ainda não prosseguiu com as avaliações para tanto. O mesmo se aplica aos selos, certificados e códigos de conduta regularmente emitidos, visto que a autoridade nacional ainda não editou tais mecanismos. No entanto, muito se questiona sobre a ISO 27701 e a possibilidade de garantir a conformidade com a LGPD. A ISO 27701, que versa sobre o Sistema de Gestão de Privacidade de Informação, é o novo padrão da família 27000, que trata sobre a segurança da informação.

Todavia, a ISO 27701 envolve uma série de regras normatizadoras de conduta e processos de caráter internacional, não sendo reconhecida pela ANPD como certificado. Nesse quesito, é importante ressaltar que, embora a ISO 27701 possa evoluir para uma norma ou padrão de certificação para leis de privacidade, a LGPD não exige conformidade em nenhuma

---

[63] TOMADA de Subsídios sobre Transferências Internacional. **Gov.br**, 2022. Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Acesso em: 27 mar. 2023.

norma internacional. Desse modo, embora não seja uma certificação reconhecida, a ISO 27701 pode ajudar no processo de adequação à legislação brasileira, encurtando a jornada de compliance com a lei.

Para finalizar as previsões legais, cabe tratar sobre o art. 36, último artigo do capítulo V da LGPD, o qual já foi mencionado previamente. Tal artigo aborda as alterações nas garantias referentes à conformação aos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 da mesma Lei. Sendo assim, quando houver alterações, a autoridade nacional deve ser comunicada, de modo que "qualquer alteração posterior sem a devida comunicação poderá invalidar a garantia, incorrendo o agente em infração da lei, sujeito às sanções cabíveis"[64].

Além dos artigos atinentes à transferência internacional de dados vistos acima, que compreendem os arts. 33 a 36 da LGPD, é necessário avaliar outras disposições, as quais podem ser utilizadas na compreensão da problemática em relação ao *cloud computing*. No que concerne ao armazenamento de dados pessoais, é assegurado ao titular que seus dados sejam armazenados em formato que favoreça o exercício do direito de acesso a eles, conforme previsão do art. 19, § 1º, da LGPD.

Outro ponto que merece destaque é a questão da responsabilidade em caso de descumprimento das previsões da Lei em questão. Nesse quesito, a LGPD trata sobre a responsabilidade nos arts. 31 e 32, no que concerne ao poder público, regido pelo sistema administrativo, e os arts. 42 a 45 do mesmo diploma legal, que versa sobre todos os agentes de proteção de dados. No caso dos órgãos públicos, conforme o art. 31, quando houver infrações, a autoridade nacional poderá enviar um relatório com as medidas cabíveis visando a cessação da violação.

Da mesma forma, a ANPD pode solicitar aos agentes do Poder Público que publiquem relatórios de impacto à proteção de dados pessoais[65], sugerindo a adoção de padrões e de boas práticas para o tratamento de tais dados, o qual foi publicado recentemente pela autoridade

---

[64] TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Comentada Artigo por Artigo. São Paulo: Editora Saraiva, 2022. *E-book*. ISBN 9786555599015. Pg. 40. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 14 jan. 2023.

[65] Existem diversos guias e modelos para a proteção de dados, os quais são disponibilizados pelo Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital no seguinte link: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd.

nacional[66], conforme previsão do art. 32 da LGPD. Segundo Patricia Peck Pinheiro[67], "o que se quer evitar é ter uma legislação que seja eficaz apenas no setor privado e não consiga ser implementada no setor público". A partir disso, deve-se tratar os arts. 42 a 45 do mesmo diploma legal, que versa sobre a responsabilidade e o ressarcimento de danos.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Em relação à responsabilidade, a LGPD se assemelhou à GDPR, visto que trouxe o caráter solidário da responsabilização do controlador e do operador. Nesse ponto, é importante tratar sobre a definição de controlador e operador, que se encontram nos incisos VI e VII, do art. 5º da Lei em voga. O controlador, como visto anteriormente, é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", enquanto o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Sendo assim, o operador (subcontratante) será responsabilizado quando não atender às determinações legais ou orientações fornecidas pelo controlador. Cabe pontuar que, caso haja mais de um controlador envolvido, todos responderão solidariamente. A LGPD trouxe a hipótese de responsabilização do operador, visto que muitos responsáveis pelo tratamento de dados se encontram em uma posição desfavorável de negociação, quando da realização de

---

[66] Para conhecer mais sobre o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, acesse: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico.

[67] PINHEIRO, Patrícia P. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021. *E-book.* ISBN 9786555595123. Pg. 40. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 20 dez. 2020.

contratos com empresas multinacionais que prestam serviços na qualidade de subcontratante, como ocorre com os grandes provedores de infraestrutura e armazenamento de dados em nuvem, que é o objeto central do presente trabalho.

Nesse aspecto, a LGPD se assemelha ao GDPR, visto que ambas tratam sobre as duas figuras. No entanto, na legislação europeia se utilizam os termos *data controller*, que é a pessoa física ou jurídica responsável por determinar as finalidades e meios a serem utilizados no processamento dos dados, e *data processor*, que é a figura que executa os atos de tratamento de dados, em nome do controlador. Como mencionado no site oficial da Comissão Europeia[68], "o processador de dados geralmente é um terceiro externo à empresa", como ocorre na figura do provedor de serviços de *cloud computing*.

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

As excludentes de responsabilidade dos agentes de tratamento exigem comprovação, uma vez que o agente é obrigado a manter tais provas sob sua custódia, em virtude do princípio da responsabilização e prestação de contas, ato conhecido como *accountability*. No entanto, ausente qualquer tipo de ilicitude, não caberá a responsabilização, o que também ocorre nos casos em que o agente não tenha tratado os dados pessoais.

O inciso III, por sua vez, trata sobre os casos de culpa exclusiva do titular dos dados ou de terceiros, que é uma hipótese de difícil comprovação. É importante dizer que algumas das previsões contidas nesses artigos têm sua correspondência no Código de Defesa do Consumidor (CDC), como ocorre com o inciso III, § 3º, do art. 12 do CDC[69]. De toda forma, para que seja aplicada essa hipótese, o agente deve comprovar que tomou todas as medidas de segurança possíveis, bem como cumpriu todas as determinações legais, sem possuir nenhuma relação com o incidente.

---

[68] Mais informações sobre o *data controller* e o *data processor* podem ser encontradas em: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en.

[69] Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
§ 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar:
I - que não colocou o produto no mercado;
II - que, embora haja colocado o produto no mercado, o defeito inexiste;
III - a culpa exclusiva do consumidor ou de terceiro.

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

É comum que, ao pensar em irregularidades no tratamento de dados, relacione-se a questão com o vazamento dessas informações. Contudo, os agentes podem ser responsabilizados por outras irregularidades, como a utilização para um fim distinto daquele concedido pelo titular. Nesse sentido, deve-se analisar o caso concreto, porque em alguns casos, a situação pode parecer irregular, mas se atendidos todos os requisitos legais e se houver a segurança adequada ao seu tratamento, o ato pode ser plenamente regular.

> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

Como mencionado anteriormente, as previsões do CDC se aplicam à proteção de dados em algumas situações, como ocorre no art. 45 da LGPD. Desse modo, encontra-se amparo na LGPD e na legislação consumerista quando da responsabilização do fornecedor em relação ao tratamento de dados do consumidor. Acerca dessa temática, pode-se falar que, em 22 de março de 2021, a ANPD assinou um acordo de cooperação técnica com a Secretaria Nacional do Consumidor (Senacon), o qual tem como principal objetivo dar agilidade nas investigações de incidentes de segurança.

A partir de toda a análise legislativa do presente subcapítulo, bem como o estudo realizado no capítulo anterior acerca do cloud computing, pode-se iniciar a análise da problemática desse sistema, que envolve principalmente a questão da segurança e proteção dos dados pessoais quando do armazenamento e transferência para servidores internacionais de computação em nuvem, principalmente no que se refere ao setor privado, que é o principal usuário dessa ferramenta. Todavia, não se deve excluir o poder público da análise, visto que o cloud computing está à disposição desse setor, como referido pelo diretor de relacionamento com clientes do Tribunal de Contas da União (TCU), Breno Costa70.

[70] O diretor de relacionamento com clientes do TCU, Breno Costa, tratou sobre a disponibilidade e aplicação do *cloud computing* pelos órgãos públicos no AWS Transformation Day, realizado em junho de 2022. No evento,

3.2 A PROBLEMÁTICA ACERCA DA TRANSFERÊNCIA E ARMAZENAMENTO DE DADOS PESSOAIS EM SERVIDORES INTERNACIONAIS DE *CLOUD COMPUTING*

A problemática do *cloud computing* em relação à transferência e armazenamento internacional de dados pessoais, operações que se enquadram como tratamento, de acordo com a definição constante do inciso X, do art. 5º, da LGPD, envolvem, principalmente, as questões atinentes à segurança do sistema. Apesar das origens do *cloud computing* se encontrarem na década de 1960, a ferramenta é relativamente nova, especialmente no que condiz à sua aplicação e aceitação no mercado, o que torna as inseguranças acerca da sua adoção algo completamente compreensível.

No entanto, como visualizado previamente, o *cloud computing* é um sistema que oferece inúmeras vantagens, especialmente no que concerne à segurança e proteção de dados. Em um país que, por muitos anos, deteve um caráter conservador frente às tecnologias, fator que advém, inclusive, do subdesenvolvimento do país, a adesão à essa ferramenta é surpreendente: de acordo com o último estudo Enterprise Cloud Index (ECI)[71], encomendado pela Nutanix, 54% dos brasileiros entrevistados afirmaram que atualmente usam várias nuvens, privadas ou públicas, como seu modelo de implantação de TI mais comum.

Além disso, segundo a mesma pesquisa, o Brasil lidera o ranking de adoção de *multicloud* no mundo, fato que impressiona, visto que o país apresenta inúmeras dificuldades para a evolução e adesão da computação em nuvem, como as questões geográficas, climáticas, energéticas e de conectividade, como visto no capítulo anterior. De toda forma, como qualquer

---

Breno falou que "organizações de governo devem olhar para a nuvem com carinho, porque podem se beneficiar bastante. Temos dificuldade de pessoal (de TI) de forma geral nos governos. E a nuvem traz um apoio grande pela automatização, pela agilidade, sem deixar de trazer inovação, benefícios de custo, de controle. Há dezenas de contratações de governo. Depois que você entra é que vai entender melhor como a nuvem pode beneficiar ainda mais. É uma plataforma adicional, que vai conviver com outras, mas que traz benefícios específicos que podemos trazer para dentro do governo". Para ler mais sobre a entrevista do diretor, acessar o seguinte link: https://www.convergenciadigital.com.br/Cloud-Computing/TCU%3A-Nuvem-compensa-falta-de-pessoal-de-TI-nos-orgaos-publicos-60474.html. No mesmo sentido, pode-se referir o GOVBRNuvem, que é a solução de *cloud computing* do governo federal em parceria com a Amazon. Para conferir mais sobre a ferramenta, veja: https://www.govbr.com.br/cloud-computing-no-servico-publico-pode-reduzir-em-80-o-custo-com-ti/#:~:text=O%20GOVBR%20Nuvem%20%C3%A9%20seguro,melhorar%20o%20atendimento%20aos%20cidad%C3%A3os.

[71] Para ler a entrevista exclusiva do country manager da Nutanix, Leonel Oliveira, acesse: https://www.convergenciadigital.com.br/Cloud-Computing/Nutanix%3A-Brasil-lidera-adocao-global-de-multicloud%2C-mas-ainda-sem-pensar-muito-no-dia-seguinte-60124.html?UserActiveTemplate=mobile.

tecnologia, existem riscos e suspeitas dos próprios usuários, visto que os vazamentos e hackeamentos de dados, bem como falhas sistêmicas são relativamente comuns.

Sendo assim, é nítida a necessidade de proteção e segurança aos dados pessoais envolvidos nesse sistema, visto que a transferência internacional é uma habitualidade na computação em nuvem, devido à localização dos servidores das empresas. Como analisado, a maioria dos servidores se localiza no continente norte-americano e europeu, embora algumas empresas já tenham servidores no Brasil, como a Google, o que reduz os riscos envolvidos na operação, além de garantir a aplicação da LGPD, uma vez que os dados permanecem em território nacional.

Portanto, a vigência da legislação de proteção de dados é tão importante, dado que ela fornece segurança aos titulares de dados pessoais, além de garantir a regularidade das empresas públicas e privadas que se utilizam dessas ferramentas. De toda forma, no que concerne ao *cloud computing*, a regulamentação dos mecanismos de transferência internacional de dados é elemento essencial. Embora a regulamentação das cláusulas-padrão contratuais esteja em desenvolvimento, os demais mecanismos de transferência também devem ser regulados para que a proteção dos dados transferidos seja completa e inequívoca.

Ademais, é necessário que as empresas adequem suas políticas à LGPD, visto que a legislação, de forma isolada, não é capaz de solucionar as questões atinentes à proteção de dados: a segurança dos dados pessoais também é uma tarefa individual. Nesse sentido, a empresa Kaspersky, em sua publicação acerca das preocupações de cibersegurança para 2023[72], pontuou que as empresas terão de combater as falhas humanas na segurança online, visando mitigar os riscos das ameaças internas, de modo que as empresas deverão investir em educação digital para os seus funcionários, visando impedir o vazamento de dados.

No que concerne à preocupação acerca dos incidentes de vazamento de dados, um mecanismo que pode ser adotado são os softwares de controle de acesso, os quais ofertam o armazenamento de dados pessoais, bem como imagens e gravações em nuvem. Tal alternativa se mostra mais segura, visto que as chaves de segurança são fornecidas conforme a necessidade de cada usuário, de modo que nem todos os agentes tenham acesso aos dados da nuvem. Os softwares de controle de acesso, embora sejam uma solução simples, reduzem a probabilidade de a empresa ter seus dados vazados.

[72] DIA da Privacidade de Dados: Kaspersky revela as preocupações de cibersegurança para 2023. **Kapersky**, 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/2023_dia-da-privacidade-de-dados-kaspersky-revela-as-preocupacoes-de-ciberseguranca-para-2023. Acesso em: 27 mar. 2023.

Além da educação digital, as empresas devem promover a sua própria adequação à LGPD, visto que esse fato contribui não somente para a reputação da empresa, como para a execução de seus contratos. Nesse sentido, cabe mencionar que as ferramentas de *cloud computing*, embora atuem disponibilizando recursos e plugins para facilitar a adequação à Lei em questão, tais sistemas não possuem o poder de, por si só, regularizar a situação da empresa no que concerne à proteção de dados.

Assim como as vantagens citadas anteriormente, o *cloud computing* adota ferramentas de controle de acesso, bem como instrumentos de monitoramento de autenticação, autorização e auditoria, o que facilita a conformidade da empresa com as normas da LGPD. Ademais, na escolha do provedor de computação em nuvem, deve-se analisar se o sistema é adequado às políticas e normas de segurança impostas pela legislação brasileira. Sendo assim, as empresas devem se atentar às certificações e padrões utilizados pelo provedor.

Por conseguinte, as empresas que já se encontram vinculadas a algum provedor de *cloud computing* devem revisar os contratos de serviços, visando garantir o cumprimento das determinações da LGPD. Como mencionado anteriormente, o provedor é o operador dos dados pessoais, enquanto a empresa que detém essas informações é a controladora. Sendo assim, em caso de irregularidade, tanto a empresa quanto o provedor podem ser responsabilizados solidariamente, conforme o art. 42, caput e § 1º, da LGPD.

Um ponto importante a ser ressaltado é que a Lei em questão possui alcance extraterritorial, uma vez que seus efeitos se estendem ao plano internacional, desde que a coleta ou a operação dos dados tenha ocorrido em território nacional (há o inciso do objetivo de fornecer os serviços no Brasil), de acordo com a previsão do art. 3º, caput e incisos, da LGPD. Nessa perspectiva, a questão levantada por Dennys Antonialli resta sanada em relação às hipóteses do artigo mencionado:

> A computação em nuvem é outro grande exemplo de incerteza quanto ao cumprimento da privacidade. Quando os usuários decidem armazenar suas informações em servidores acessíveis em todo o mundo, eles estão entregando seus dados a uma empresa que normalmente não está localizada em seu país de origem. Se seus dados são armazenados no exterior, que lei nacional deve reger as questões de privacidade: a do local onde o servidor é hospedado ou a do país onde o usuário vive? Estes são exemplos que demonstram que este é um debate bloqueado. Não há apenas uma tensão entre privacidade e controle, mas também uma tensão entre os diferentes conceitos legais nacionais de privacidade e a necessidade de cumprir com todos eles ao mesmo tempo.[73] (tradução livre)

[73] A tradução livre advém do seguinte texto original: "*Cloud computing is another great example of privacy compliance uncertainty. When users decide to store their information in servers accessible worldwide, they are giving away their data to a company which is usually not located in their home country. If their data is stored abroad, which national law should govern privacy matters: the one of the place where the server is hosted or the one of the country the user lives in? These are examples which demonstrate that this is a deadlocked debate.*

Na mesma temática de alcance da LGPD, cabe mencionar uma questão levantada pelo líder de conformidade técnica da AWS Brasil para o setor público, Fernando Gebara, em um webinar que compôs a Semana de Segurança de Dados[74]:

> A LGPD rege apenas os aspectos relativos ao processamento de dados pessoais. Toda a massa de dados de contabilidade, ou de processamentos internos, por exemplo, se não contiver dado pessoal, não é regida pela LGPD. Mas todas as organizações, especialmente a partir de um problema detectado, têm que demonstrar que adotou aspectos de segurança, procedimentos, processos, que comprovem que estava agindo da melhor forma possível, incluindo demonstrar a eficácia dessas medidas. Determinar quem fez acesso, quando os acessos ocorreram, por exemplo, são aspectos que as empresas precisam demonstrar que são capazes de fazer.

Portanto, a adequação às leis de proteção de dados é tão crucial no mundo tecnológico que vivemos hoje. Segundo projeções, mais de 80% dos novos aplicativos corporativos usarão a nuvem como plataforma até 2025[75]. Tal fato já se mostra verdade, visto que os principais sistemas de streaming, como a Netflix, utilizam o *cloud computing*, o que demonstra uma tendência global de utilização dessas ferramentas. Sendo assim, a aceitação desse modelo tanto pelas empresas como pelos governos deve ser, pelo menos, objeto de discussão, visto que tais medidas podem facilitar as conexões transfronteiriças e, consequentemente, ampliar as relações comerciais existentes.

As leis existentes anteriormente não eram abrangentes, de modo que ofereciam somente a implantação de padrões mínimos aos Estados, o que resultava em padrões inadequados de proteção de dados e, consequentemente, em uma maior insegurança acerca da adoção das tecnologias de nuvem. Contudo, conforme exposto, essa realidade foi alterada, de modo que, atualmente, existam leis específicas em cada país, como é o caso da LGPD no Brasil e da GDPR na União Europeia. Por conta disso, o presente trabalho se pautava em duas hipóteses: i) a viabilidade da minimização de dados; e ii) a impossibilidade de minimizar os dados envolvidos nessas operações.

There is not only a tension between privacy and control but also a tension between the different national legal concepts of privacy and the necessity to comply with all of them at the same time". (ANTONIALLI, Dennys. *Privacy and international compliance: when differences become an issue*. 2010. Disponível em: https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1165/1470).

[74] GROSSMAN, Luís Osvaldo. AWS: TI tem de estar atenta à LGPD e aos papéis do cliente e do provedor de nuvem. **Convergência Digital**, 2021. Disponível em: https://www.convergenciadigital.com.br/Cloud-Computing/AWS%3A-TI-tem-de-estar-atenta-a-LGPD-e-aos-papeis-do-cliente-e-do-provedor-de-nuvem-56094.html?UserActiveTemplate=mobile. Acesso em: 27 mar. 2023.

[75] A projeção se encontra em artigo disponibilizado na Revista Ibérica de Sistemas e Tecnologias de Informação. É possível acessar o artigo no seguinte link: https://www.researchgate.net/profile/Marcio-Fernandes-12/publication/358982951_Impactos_da_Lei_de_Protecao_de_Dados_LGPD_brasileira_no_uso_da_Computacao_em_Nuvem/links/6220d9c7801c9229105585e9/Impactos-da-Lei-de-Protecao-de-Dados-LGPD-brasileira-no-uso-da-Computacao-em-Nuvem.pdf.

A primeira hipótese pode ser vista, por aqueles que possuem um pensamento desconfiado frente à segurança envolvida nas tecnologias, como uma credibilidade excessiva. No entanto, esse pensamento está muito mais atrelado a uma crença conservadora de que o universo digital apresenta perigos em toda e qualquer utilização, concepção reforçada pelos noticiários que, ao tratar sobre dados pessoais, acabam reforçando a sua face negativa. Nesse sentido, dizer que as operações de transferência e armazenamento internacional de dados pessoais não envolvem riscos é algo irreal, visto que, conforme analisado ao longo do trabalho, esses procedimentos são, por essência, arriscados.

Todavia, o desenvolvimento de ferramentas que minimizem esses riscos é cada vez maior: tanto a criação de legislações específicas para a proteção de dados, quanto o aprimoramento das estruturas de segurança resultam em um movimento convergente, no que concerne a redução dos perigos envolvidos nos sistemas de computação em nuvem. Além disso, o *cloud computing* se mostrou um forte aliado ao Direito e, consequentemente, à proteção de dados pessoais, visto que possibilitam uma adequação mais rápida à LGPD, bem como demonstraram ser mais eficientes e, em certa medida, mais seguros do que a computação local, embora ainda haja receio na utilização dessas ferramentas.

Sendo assim, a segunda hipótese levantada restou vencida em comparação à primeira, embora tenha suas razões de existência. Dessa forma, além das políticas, legislações e ferramentas de segurança, é necessária uma mudança de mentalidade na sociedade como um todo, uma vez que as ferramentas de tecnologia, embora sejam comprovadamente nocivas, devem ser tidas como facilitadoras do cotidiano, principalmente quando tratamos de quantidades expressivas de informações, como ocorre na maioria das empresas, visto que os dados pessoais estão presentes nas mais diversas relações.

4 CONCLUSÃO

No mundo globalizado em que vivemos, em que se estima que 60% do PIB mundial é digitalizado[76], o fluxo de comunicações, dados e informações ocorre de forma contínua e instantânea. Nesse sentido, a transferência de dados ocorre tanto na esfera pública quanto na privada. O poder público, as empresas privadas e os próprios indivíduos são agentes diretos do compartilhamento de dados e, por tal motivo, adotar modelos burocráticos e inflexíveis pode ser um impeditivo para as mais diversas formas de desenvolvimento, como por exemplo, tecnológico e econômico.

O uso de infraestruturas tecnológicas, como o *cloud computing*, impõe a transferência internacional habitual de dados pessoais, visto que os servidores onde tais informações ficam armazenadas se localizam, em muitos casos, no exterior. É importante ressaltar que o uso dessas ferramentas tecnológicas não é algo exclusivo das grandes empresas, uma vez que esses sistemas são flexíveis e, consequentemente, abarcam todos os tipos de empresa e de patrimônio disponível para a sua adoção, incluindo, como referido anteriormente, os órgãos públicos.

Uma crítica feita por Marcel Leonardi é que a interpretação restritiva dos dispositivos sobre a transferência internacional de dados pessoais "pode colocar a LGPD em completo descompasso com a dinâmica da economia moderna e do uso de serviços on-line pelos próprios titulares desses dados"[77]. No entanto, pelo exposto no presente trabalho, entende-se que a legislação brasileira é um instrumento legal que abrange inúmeras possibilidades de transferência internacional, sem permitir que a segurança e a proteção dos dados pessoais sejam corrompidas, tendo em vista a sua inspiração na GDPR, que é tida como a legislação de proteção de dados e segurança mais rígida do mundo.

No entanto, diversos pontos devem ser desenvolvidos no Brasil em relação à computação em nuvem. Conforme Henrique Cecci, mencionado anteriormente neste trabalho, o Brasil tem alguns desafios a serem enfrentados, os quais envolvem a centralização das ofertas de nuvem em grandes centros urbanos, como o Rio de Janeiro e São Paulo, e o custo local de *cloud*, o qual é 78% maior do que nos Estados Unidos[78]. De toda forma, Cecci pontua que, com

---

[76] OVERSTRAETEN, Tanguy Van. Cross-border data flows: A necessary part of global trade. **AmCham**, 2021. Disponível em: https://www.amchameu.eu/blog/cross-border-data-flows-necessary-part-global-trade. Acesso em: 27 mar. 2023.

[77] BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200. Pg. 309. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 23 dez. 2023.

[78] REDAÇÃO da Abranet. Brasil ainda é imaturo no uso de computação em nuvem. **Abranet**: Associação Brasileira de Internet, 2022. Disponível em: https://www.abranet.org.br/Noticias/Brasil-ainda-e-imaturo-no-uso-de-computacao-em-nuvem-

a ampliação das redes de 5G, a necessidade de pequenos data centers distribuídos pelo país poderá auxiliar o desenvolvimento do *cloud computing*, visto que tais tecnologias necessitam do sistema de nuvem. Nesse sentido, o diretor sênior do Grupo Gartner afirma que

> Essas plataformas possibilitam crescimento e transformação de negócios, entregando resultados rápidos por meio de serviços existentes. Por isso (o mercado) vem crescendo de forma rápida. E as empresas estão aprendendo a identificar o valor: hoje não existe estratégia de negócio sem estratégia de *cloud*.

Ademais, é importante mencionar que, além dos fatores climáticos, energéticos e de conectividade, a regulação presente no país é determinante na escolha da localização dos servidores. Desse modo, o aspecto tributário, principalmente no que se refere aos incentivos fiscais, e a normatização envolvendo a proteção de dados devem ser tratadas em conjunto em relação a tais tecnologias. Nesse sentido, cabe pontuar que a questão econômico-fiscal é uma das mais importantes, visto que nos países em que as tributações são reduzidas, há maior inserção de servidores, como ocorreu com a Irlanda, exemplo mencionado anteriormente. Sendo assim, é necessário um esforço governamental para que as empresas sejam atraídas para o Brasil.

Embora o cenário seja promissor, ainda existem muitos obstáculos a serem enfrentados: um estudo da Surfshark, companhia holandesa de cibersegurança já citado no presente trabalho, atestou que o Brasil é o 4º país do mundo que mais apresentou casos de usuários violados com vazamento de dados no segundo trimestre de 2022[79], assumindo essa posição pelo segundo trimestre seguido. Sendo assim, não é estranho que ainda haja empresas que escolham a computação local, visto que, nesse sistema, há um controle total dos dados pessoais sob custódia das companhias, o que oferece, pelo menos em tese, uma maior segurança. Contudo, deve-se ter em mente que, cada vez mais, os sistemas de *cloud computing* apresentam inovações e vantagens que, em suma, superam os seus pontos negativos.

Por todo o exposto, é possível responder à questão basilar do presente trabalho, que trata sobre a possibilidade de minimização dos riscos nessa operação, mediante a definição e a aplicação de critérios particularizados, que devem ser controlados e fiscalizados pelas próprias empresas e pela Autoridade Nacional de Proteção de Dados. Nesse sentido, conclui-se que a legislação nacional é apta para reduzir os riscos operacionais relativos ao *cloud computing*,

---

3983.html?UserActiveTemplate=site&UserActiveTemplate=mobile#.Y9HqX3bMLrc. Acesso em: 27 mar. 2023.

[79] VILELA, Luiza. Cibersegurança: 459 brasileiros têm seus dados vazados a cada 60 segundos. **Consumidor Moderno**, 2022. Disponível em: https://www.consumidormoderno.com.br/2022/07/19/brasileiros-dados-vazados-segundos/. Acesso em: 27 mar. 2023.

visto que cada mecanismo de transferência internacional de dados será propriamente analisado e deverá passar pelo crivo da autoridade nacional, de forma que as irregularidades serão puníveis de acordo com as previsões existentes.

No entanto, deve-se relembrar a necessidade das empresas de se adequarem à LGPD, sejam elas públicas ou privadas. Portanto, a minimização dos riscos é um esforço conjunto entre a autoridade nacional, responsável pela implementação e fiscalização do cumprimento da Lei em todo território nacional, e cada um dos agentes de tratamento de dados pessoais, visto que tanto os controladores quanto os operadores devem estar atuando de forma compatível com a legislação nacional, uma vez que são responsáveis solidariamente pelas obrigações referentes ao tratamento dos dados que se encontram sob sua custódia.

Por fim, é necessário pontuar que, embora os agentes de tratamento sejam os principais responsáveis pelos dados pessoais que se encontram mantidos sob seu poder, os titulares desses dados também devem se manter informados e conscientes acerca da localização e utilização das informações que são concedidas. Segundo pesquisa da Kaspersky[80], empresa de cibersegurança já abordada no presente trabalho, cerca de 40% dos brasileiros desconhecem os meios pelos quais seus dados são coletados. Nesse sentido, a temática da proteção de dados, de maneira geral, deve ser retirada do ambiente acadêmico e corporativo para adentrar em outras esferas, alcançando toda sociedade, visto que um maior conhecimento acerca dos dados pessoais pode evitar incidentes futuros.

[80] A pesquisa completa pode ser encontrada no seguinte link: https://www.kaspersky.com.br/blog/pesquisa-impressoes-digitais/18906/.

REFERÊNCIAS

AGÊNCIA Senado. Punições pelo uso indevido de dados pessoais começam a valer no domingo. **Senadonotícias**, 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo. Acesso em: 27 mar. 2023.

ANTEPROJETO de Lei de Proteção de Dados para segurança pública e persecução penal. **Comissão de Juristas**, 2019. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 17 fev. 2023.

BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 23 dez. 2023.

BRASIL é o 6º país com o maior número de vazamentos de dados. **Terra**, 2022. Disponível em: https://www.terra.com.br/noticias/brasil-e-o-6-pais-com-o-maior-numero-de-vazamentos-de-dados,3e719e5dc73f1f2c6036ffa694b938cd2y9nf8qi.html#:~:text=Os%20Estados%20Unidos%20ocupam%20o,%2C%20com%2086%2C6%20milh%C3%B5es. Acesso em: 23 mar. 2023.

BRASIL é o País da América Latina que mais utiliza e investe em cloud. *Itforum*, 2018. Disponível em: https://itforum.com.br/noticias/brasil-e-o-pais-da-america-latina-que-mais-utiliza-e-investe-em-cloud/. Acesso em: 27 mar. 2023.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. DF: Brasília, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 23 mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). DF: Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 mar. 2023.

CHEUNG, Anne S. Y.; WEBER, Rolf H. (orgs.). **Privacy and Legal Issues in Cloud Computing**. Cheltenham: Edward Elgar Publishing, 2016.

CLOUD Adoption & Risk Report. **McAfee**, 2019. Disponível em: https://cts.businesswire.com/ct/CT?id=smartlink&url=https://www.skyhighnetworks.com/cloud-computing-trends-2019/&esheet=51890399&newsitemid=20181029005552&lan=en-US&anchor=Cloud+Adoption+&+Risk+Report+Landing+Page&index=2&md5. Acesso em: 02 jan. 2023.

CNN Brasil Business. Entenda o que é o imposto mínimo global apoiado por líderes do G20. **CNN Brasil**, 2021. Disponível em: https://www.cnnbrasil.com.br/business/entenda-o-que-e-o-imposto-minimo-global-apoiado-por-lideres-do-g20/#:~:text=A%20taxa%20de%2015%25%20ser%C3%A1,%24%20845%20bilh%C3%B5es)%20por%20ano. Acesso em: 27 mar. 2023.

COHEN, Jason. 4 Companies Control 67% of the World's Cloud Infrastructure. **PCMag**, 2021. Disponível em: https://www.pcmag.com/news/four-companies-control-67-of-the-worlds-cloud-infrastructure. Acesso em: 27 mar. 2023.

COMER, Douglas E. **Redes de Computadores e Internet**. Porto Alegre: Bookman, 2016. E-book. ISBN 9788582603734. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788582603734/. Acesso em: 25 fev. 2023.

COMISSÃO EUROPEIA**. Cláusulas contratuais padrão para transferências internacionais**. União Europeia, 2021. Disponível em: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en. Acesso em: 20 fev. 2023.

DIA da Privacidade de Dados: Kaspersky revela as preocupações de cibersegurança para 2023. **Kapersky**, 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/2023_dia-da-privacidade-de-dados-kaspersky-revela-as-preocupacoes-de-ciberseguranca-para-2023. Acesso em: 27 mar. 2023.

DOBLAS, Beatriz. O maior vazamento de dados da história mostra que usar sistema em Nuvem é essencial. **Nasajon**, 2021. Disponível em: https://nasajon.com.br/o-maior-vazamento-de-dados-de-historia-mostra-que-usar-sistema-em-nuvem-e-essencial/. Acesso em: 27 mar. 2023.

DOUBLE Irish with a Dutch Sandwich: Definition and How It`s Used. **Investopedia**, 2020. Disponível em: https://www.investopedia.com/terms/d/double-irish-with-a-dutch-sandwich.asp. Acesso em: 11 abr. 2023.

ESPECIALISTAS Inmetrics. Cloud Computing: como a pandemia acelerou a implementação. **Inmetrics**, [202?]. Disponível em: https://inmetrics.com.br/blog/cloud-computing-como-a-pandemia-acelerou-a-implementacao/. Acesso em: 27 mar. 2023.

FERNANDES, Márcio Aurélio de Souza et al. Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da Computação em Nuvem. **RISTI**, n. E42, 2021. Disponível em: https://www.researchgate.net/profile/Marcio-Fernandes-12/publication/358982951_Impactos_da_Lei_de_Protecao_de_Dados_LGPD_brasileira_no_uso_da_Computacao_em_Nuvem/links/6220d9c7801c9229105585e9/Impactos-da-Lei-de-Protecao-de-Dados-LGPD-brasileira-no-uso-da-Computacao-em-Nuvem.pdf. Acesso em: 23 mar. 2023.

FUNDAÇÃO GETULIO VARGAS. **Guia de Proteção de Dados Pessoais - Transferência Internacional**. Versão 1.0, Outubro, 2020, p. 13. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/transferencia_internacional.pdf . Acesso em: 23 fev. 2023

GENERAL Data Protection Regulation (GDPR). **GDPR.EU**, [202?] Disponível em: https://gdpr.eu/tag/gdpr/. Acesso em: 23 mar. 2023.

GLOBAL Cloud Computing Market Size & Share Will Reach USD 1025.9 Billion by 2026: Facts & Factors. **GlobeNewswire**, 2021. Disponível em: https://www.globenewswire.com/news-release/2021/01/22/2162789/0/en/Global-Cloud-

Computing-Market-Size-Share-Will-Reach-USD-1025-9-Billion-by-2026-Facts-Factors.html#:~:text=%E2%80%9CAccording%20to%20the%20research%20study,%25%20from%202019%20to%202027%E2%80%9D. Acesso em: 27 mar. 2023.

GROSSMAN, Luís Osvaldo. AWS: TI tem de estar atenta à LGPD e aos papéis do cliente e do provedor de nuvem. **Convergência Digital**, 2021. Disponível em: https://www.convergenciadigital.com.br/Cloud-Computing/AWS%3A-TI-tem-de-estar-atenta-a-LGPD-e-aos-papeis-do-cliente-e-do-provedor-de-nuvem-56094.html?UserActiveTemplate=mobile. Acesso em: 27 mar. 2023.

GUIAS e modelos. **Governo Digital**, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em: 23 mar. 2023.

HISTÓRIA da computação em nuvem: como surgiu a cloud computing? **IPM**, 2020. Disponível em: https://www.ipm.com.br/blog/administracao-geral/historia-da-computacao-em-nuvem-como-surgiu-a-cloud-computing/https://www.ipm.com.br/blog/administracao-geral/historia-da-computacao-em-nuvem-como-surgiu-a-cloud-computing/. Acesso em: 27 mar. 2023.

KANADE, Vijay. Cloud vs. On-Premise Comparison: Key Differences and Similarities. **Spiceworks**, 2021. Disponível em: https://www.spiceworks.com/tech/cloud/articles/cloud-vs-on-premise-comparison-key-differences-and-similarities/. Acesso em: 27 mar. 2023.

KANADE, Vijay. Top 10 Cloud Security Challenges to Overcome in 2021. **Spiceworks**, 2021. Disponível em: https://www.spiceworks.com/it-security/cloud-security/articles/top-cloud-security-challenges/. Acesso em: 27 mar. 2023.

LGPD e Cloud Computing: acelere a sua jornada de adequação à Lei. **HSBS**, [202?]. Disponível em: https://www.hsbs.com.br/blog-lgpd-e-cloud-computing/. Acesso em: 23 mar. 2023.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados**. (Coleção teses de doutoramento). São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584936397. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 19 dez. 2022.

LIMA, Matheus Araújo Campi; SILVA, Matheus Melo da. Dos Crimes de Invasão e Vazamento de dados, frente à Legislação Brasileira. **Jusbrasil**, 2021. Disponível em: https://matheusmelos.jusbrasil.com.br/artigos/1227878101/dos-crimes-de-invasao-e-vazamento-de-dados-frente-a-legislacao-brasileira#:~:text=Podemos%20considerar%20que%20a%20primeira,154%2DA%20no%20C%C3%B3digo%20Penal. Acesso em: 27 mar. 2023.

MARINHO, Fernando. **Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos**. São Paulo: Grupo GEN, 2020. E-book. ISBN 9788597026009. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788597026009/. Acesso em: 04 de jan. 2023.

MEGAVAZAMENTO de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 27 mar. 2023.

MOHANAKRISHNAN, Ramya. What Is Cloud Computing Security? Definition, Risks, and Security Best Practices. **Spiceworks**, 2021. Disponível em: https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing-security/. Acesso em: 27 mar. 2023.

NEW Statistics Show the Advance of Cloud Computing. **Eukhost**, 2020. Disponível em: https://www.eukhost.com/blog/webhosting/new-statistics-show-the-advance-of-cloud-computing/. Acesso em: 27 mar. 2023.

NO DIA Internacional da Proteção de Dados, ANPD publica Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público. **Autoridade Nacional de Proteção de Dados**, 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico. Acesso em: 23 mar. 2023.

NÚCLEO de Informação e Coordenação do Ponto BR [edit.]. **Privacidade e proteção de dados pessoais 2021**: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 27 mar. 2023.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. **OECD**: Organisation for Economic Co-operation and Development, 2002. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 23 fev. 2023.

OLIVEIRA, Marcela. Desdobramentos da LGPD Penal. **LGPDbrasil,** 2022. Disponível em: https://www.lgpdbrasil.com.br/desdobramentos-da-lgpd-penal/. Acesso em: 27 mar. 2023.

O QUE é infraestrutura de nuvem? **Redhat**, 2019. Disponível em: https://www.redhat.com/pt-br/topics/cloud-computing/what-is-cloud-infrastructure. Acesso em: 27 mar. 2023.

O QUE é o Secure Access Service Edge (SASE)? **Cisco**, [202?]. Disponível em: https://www.cisco.com/c/pt_br/products/security/what-is-sase-secure-access-service-edge.html#~resumo-de-sase. Acesso em: 27 mar. 2023.

O QUE significa arquivar na nuvem? Onde ficam os principais servidores? **Tiltuol**, 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/05/01/o-que-significa-arquivar-na-nuvem-onde-ficam-os-principais-servidores.htm. Acesso em: 27 mar. 2023.

OVERSTRAETEN, Tanguy Van. Cross-border data flows: A necessary part of global trade. **AmCham**, 2021. Disponível em: https://www.amchameu.eu/blog/cross-border-data-flows-necessary-part-global-trade. Acesso em: 27 mar. 2023.

PATIL, Prajakta; BASUMALLICK, Chiradeep. What is Cloud Computing? Definition, Benefits, Types, and Trends. **Spiceworks**, 2022. Disponível em:

https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/. Acesso em: 27 mar. 2023.

PESQUISA: Impressões Digitais e sua relação com as pessoas e as empresas. **Cibersegurança,** 2022. Disponível em: https://www.kaspersky.com.br/blog/pesquisa-impressoes-digitais/18906/. Acesso em: 23 mar. 2023.

PESQUISA mostra que Rússia, China, EUA e Brasil são os países que mais atacaram a América Latina no segundo semestre de 2020. **Terra,** 2021. Disponível em: https://www.terra.com.br/noticias/dino/pesquisa-mostra-que-russia-china-eua-e-brasil-sao-os-paises-que-mais-atacaram-a-america-latina-no-segundo-semestre-de-2020,f542782745c862aca4b749bdac0b2d1ezjndffzu.html. Acesso em: 27 mar. 2023.

PINHEIRO, Patrícia P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555595123. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 20 dez. 2020.

PROJEÇÃO da população do Brasil e das Unidades da Federação. **IBGE**: Instituto Brasileiro de Geografia e Estatística, 2023. Disponível em: https://www.ibge.gov.br/apps/populacao/projecao/. Acesso em: 27 mar. 2023.

REDAÇÃO da Abranet. Brasil ainda é imaturo no uso de computação em nuvem. **Abranet**: Associação Brasileira de Internet, 2022. Disponível em: https://www.abranet.org.br/Noticias/Brasil-ainda-e-imaturo-no-uso-de-computacao-em-nuvem-3983.html?UserActiveTemplate=site&UserActiveTemplate=mobile#.Y9HqX3bMLrc. Acesso em: 27 mar. 2023.

RELAÇÃO entre ISO 27701 e a LGPD: o que você precisa saber. **Microservice**, [202?]. Disponível em: https://www.microserviceit.com.br/relacao-entre-iso-27701-e-lgpd-o-que-voce-precisa-saber/. Acesso em: 27 mar. 2023.

TAVARES, Lucas. Hospedagem Cloud. **Melhores Hospedagem**, 2023. Disponível em: https://www.melhoreshospedagem.com/hospedagem-cloud/. Acesso em: 23 mar. 2023.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Comentada Artigo por Artigo. São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555599015. Disponível em: https://app.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 14 jan. 2023.

THE world's most valuable resource is no longer oil, but data. **The Economist**, Londres, 06 de maio de 2017. Disponível em: https://econ.st/3oeRM7G. Acesso em: 26 fev. 2022.

UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. [1995]. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Acesso em: 23 fev. 2023.

UNIÃO EUROPEIA. **Convention 108 of the Council of Europe for the protection of individuals with regard to the processing of personal data**. Disponível em

https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/C onvention_108_EN.pdf. Acesso em 23 fev. 2023.

VARON, Joana. Transferência Internacional de Dados. **Comissão Especial da Câmara de Deputados**, 2016. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/55a-legislatura/pl-4060-12-tratamento-e-protecao-de-dados-pessoais/documentos/audiencias-e-eventos/joana-varon. Acesso em: 22 jan. 2023.

VILELA, Luiza. Cibersegurança: 459 brasileiros têm seus dados vazados a cada 60 segundos. **Consumidor Moderno**, 2022. Disponível em: https://www.consumidormoderno.com.br/2022/07/19/brasileiros-dados-vazados-segundos/. Acesso em: 27 mar. 2023.