CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

GOVERNANÇA SUSTENTÁVEL II

MÁRCIO LUÍS DE OLIVEIRA

THIAGO LOURES MACHADO MOURA MONTEIRO

HUMBERTO GOMES MACEDO

G721
Governança sustentável II [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Márcio Luís de Oliveira, Thiago Loures Machado Moura Monteiro e Humberto Gomes Macedo – Belo Horizonte: Skema Business School, 2020.

Inclui bibliografia
ISBN: 978-65-5648-095-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Desafios da adoção da inteligência artificial no campo jurídico.
1. Direito. 2. Inteligência Artificial. 3. Tecnologia. I. Congresso Internacional de Direito e Inteligência Artificial (1:2020 : Belo Horizonte, MG).

CDU: 34

CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

GOVERNANÇA SUSTENTÁVEL II

Apresentação

É com enorme alegria que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 14 livros produzidos a partir dos Grupos de Trabalho do I Congresso Internacional de Direito e Inteligência Artificial. As discussões ocorreram em ambiente virtual ao longo dos dias 02 e 03 de julho de 2020, dentro da programação que contou com grandes nomes nacionais e internacionais da área, além de 480 pesquisadoras e pesquisadores inscritos no total. Estes livros compõem o produto final deste que já nasce como o maior evento científico de Direito e da Tecnologia do Brasil.

Trata-se de coletânea composta pelos 236 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os quatro Grupos de Trabalho originais, diante da grande demanda, se transformaram em 14 e contaram com a participação de pesquisadores de 17 Estados da federação brasileira. São cerca de 1.500 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre os temas Direitos Humanos na era tecnológica, inteligência artificial e tecnologias aplicadas ao Direito, governança sustentável e formas tecnológicas de solução de conflitos.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 41 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, certamente, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para ensino e pesquisa de excelência no universo da economia do conhecimento. A SKEMA, cujo nome é um acrônimo significa School of Knowledge Economy and Management, acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Até 2021, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 07 de agosto de 2020.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs

Coordenador Acadêmico da Pós-graudação de Direito e Inteligência Artificial da SKEMA Business School

STANDARDS MÍNIMOS À CONTRATAÇÃO DE CLOUD SERVICE PELO PODER PÚBLICO: ESTUDOS PRELIMINARES

BASIC STANDARDS FOR CLOUD SERVICE CONTRACTS BY THE PUBLIC ADMINISTRATION: PRELIMINARY STUDIES

Isadora Formenton Vargas [1]
Matheus Linck Bassani [2]

Resumo

O problema de pesquisa envolve identificar standards mínimos para a contratação de serviços de nuvem pelo Poder Público, a partir das iniciativas brasileiras atuais. A partir do método dedutivo, bases legais e alguns critérios de contratação são apresentados, que deverão ser objeto de inúmeras abordagens pelos Tribunais brasileiros. Conclui-se a necessidade de que os contratantes procedam a um aprofundado planejamento prévio e contínuo, em razão dos diversos modelos de serviço de cloud service, que garantam tanto a segurança dos dados, quanto a transparência necessárias à proteção da soberania nacional em relação à governança digital e de dados.

Palavras-chave: Governança digital, Proteção de dados, Contrato, Armazenamento em nuvem

Abstract/Resumen/Résumé

The research problem involves identifying basic standards cloud services contracts by the Brazilian Government, based on current initiatives. Based on the deductive method, legal bases and some hiring criteria are presented, which should be the subject of numerous approaches by the Brazilian Courts. For conclusion, it was possible to identify the need for contractors to carry out prior and continuous planning in-depth due to the various cloud service models offered in the market, which guarantee both the security of data and the transparency necessary to protect national sovereignty in relation to digital and data governance.

Keywords/Palabras-claves/Mots-clés: Digital governance, Cloud services, Data protection, Contract

[1] Mestre em Argumentação Jurídica (Universidade de Alicante e de Palermo). Mestranda em Direito (UFRGS).

[2] Doutor e Mestre em Direito (UFRGS).

1. Introdução

A governança digital busca tornar o Estado mais eficiente, dinâmico e competitivo. Atualmente, a governança de dados possui um papel relevante no que se denomina uma nova compreensão de "soberania nacional". No entanto, surgem desafios que merecem atenção: impactos da governança algorítmica, necessidade de mecanismos de segurança dos dados, adequação, minimização e criptografia dos dados, por exemplo. Dentre os serviços que compõem a implementação dessas tecnologias, encontra-se o armazenamento em nuvem (*cloud*).

De acordo com a Estratégia Brasileira para a Transformação Digital, busca-se "aprimorar a infraestrutura de redes e bancos de dados da Administração Pública Federal, promovendo a migração do modelo de armazenamento para dados em nuvem, e ampliando a inteligência e cruzamento de bases de dados" (GOVERNO FEDERAL, 2018, p. 103). Para promover essas mudanças, o Poder Público tende a contar com atores privados, uma vez que não possui interesse em prover esse serviço.

Nesse sentido, o Serviço Federal de Processamento (SERPRO) - que se encontra na lista da privatização do Ministério da Economia -, por meio da Consulta Pública Eletrônica nº 1863, em novembro de 2019, anunciou a busca por provedores de serviços em nuvem nas modalidades Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). Em 02 de junho de 2020, veio a público a contratação da Amazon Web Services para prestação dos serviços em nuvem (SERPRO, 2020).

Em 27 de maio de 2020, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) anunciou um acordo de colaboração "Acelerando a Transformação Digital" (MCTIC, 2020) com a empresa CISCO, que, recentemente, pagou multa de US$ 8,6 milhões por vender tecnologia de vigilância com falhas graves de segurança e vulnerabilidades de alto risco (BENNER; CONGER, 2019).

Em 12 de junho de 2020, o Ministério da Economia publicou a Consulta Pública nº 04/2020, cujo objeto consiste no Registro de Preços para eventual contratação de empresa especializada para prestação de serviços gerenciados de computação em nuvem, sob o modelo de cloud broker (integrador) de multi nuvem, que inclui a concepção, projeto, provisionamento, configuração, migração, suporte, manutenção e gestão de topologias de serviços em dois ou mais provedores de nuvem pública (MINISTÉRIO DA ECONOMIA, 2020), o que confirma a atualidade e pertinência do tema.

A problemática emerge a partir da identificação de que os dados a serem armazenados são ativos extremamente relevantes por sua natureza sensível, de titularidade de milhares de brasileiros, o que leva à necessária atenção aos riscos exponenciais da governança digital e de dados. Sem desconsiderar os benefícios, que buscam a desburocratização e otimização das políticas públicas, mediante método dedutivo, fundado em fontes nacionais e estrangeiras, questiona-se os critérios ou *standards* mínimos à contratação de serviço de armazenamento em nuvem (*cloud service)* pelo Poder Público.

A hipótese da pesquisa é que a discricionariedade em contratar está adstrita à garantia que os dados estarão seguros respeitando o princípio da privacidade dos cidadãos e de que as informações sensíveis, tanto privadas como públicas - de segurança nacional - estarão livres de qualquer interferência. De forma sucinta, serão expostas as normas aplicáveis e, posteriormente, alguns requisitos a serem observados nesse tipo de contratação. Ao final, serão tecidas as considerações finais.

2. Contexto jurídico

A Governança de Dados, de acordo com o Governo Federal, consiste no "planejamento, monitoramento e execução, sobre a gestão de ativos de dados de modo a promover interoperabilidade das informações, meio de análise de políticas públicas e serviços digitais mais simples e ágeis ao cidadão, organizações e empresas" (GOVERNO DIGITAL, *online*).

A viabilizar a governança digital, uma série de decretos foram publicados, dentre eles, o Decreto nº 10.046/2019, o qual dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados (BRASIL, 2019). Nos incisos do art. 2º do referido decreto, faz-se referência a uma série de dados sensíveis: atributos biográficos, biométricos e dados cadastrais, quanto a esses últimos, podem vir a se tornar sensíveis a depender do contexto e finalidade de uso.

Anteriormente, vigorava o Decreto nº 8.936/2016, revogado pelo Decreto nº 10.332/2020, que instituiu a Estratégia de Governo Digital para o período de 2020 a 2022 no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Consta, dentre os objetivos a serem alcançados: "adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal".

O Decreto nº 10.332/2020 também estabelece, no anexo, a "iniciativa 16.5" que consiste na "migração de serviços de, pelo menos, trinta órgãos para a nuvem, até 2022". Ademais, o Decreto prevê "implementar recursos para criação de uma rede de blockchain do Governo federal interoperável", e visa também ao fornecimento de "serviços preditivos e personalizados ao cidadão", referindo, na mesma oportunidade, "um governo confiável, que respeita a liberdade e a privacidade dos cidadãos e assegura resposta adequada aos riscos, ameaças e desafios que surgem com o uso das tecnologias digitais no Estado".

A preocupação que emerge se refere à materialização da proteção de dados, a exemplo dos desafios encontra-se o tratamento preditivo, que pode gerar a manutenção de discriminações arbitrárias. No caso, o Decreto nº 10.332/2020 expressamente determina, como objetivo: "estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020" e, também, "estabelecer plataforma de gestão da privacidade e uso dos dados pessoais do cidadão, até 2020".

Em 14 de abril de 2020, anterior ao Decreto nº 10.332/2020, foi publicada a Resolução nº 4, que disponibiliza o Guia de Boas Práticas para Implementação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) na Administração Pública Federal. Ocorre que, embora mencione a atualização e aperfeiçoamento, conforme diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), esse órgão ainda não foi criado, embora a LGPD já vigorasse quanto à implementação da autoridade desde 2018.

O Guia de Boas Práticas de Proteção de Dados, de março de 2020, aponta, no que tange ao armazenamento em nuvem, o relacionamento do ciclo de vida do tratamento dos dados pessoais com ativos organizacionais. Na fase de retenção, "deve-se avaliar os ativos utilizados para armazenar os dados pessoais. Esses dados podem estar armazenados em bases de dados, documentos físicos, equipamentos ou sistemas" (GOVERNO FEDERAL, 2020, p. 43). Nesse sentido, indica que, caso o serviço de armazenamento seja em nuvem, "é necessário considerar o serviço de armazenamento contratado e/ou utilizado" (GOVERNO FEDERAL, 2020, p. 43).

Em que pese a existência de guia de boas práticas, com importantes considerações a respeito da segurança da informação, inclusive com a previsão de privacidade desde a concepção e por padrão (GOVERNO FEDERAL, 2020, p. 46), percebe-se que há desafios referentes à fiscalização de contratações entre Poder Público e entidades privadas, no que tange à implementação das tecnologias necessárias à governança digital.

De acordo com a legislação aplicável ao Edital do SERPRO, verifica-se a dispensa de licitação prevista no inciso II, §3º, do art. 28, da Lei nº 13.303/2016 (Lei das Estatais), que viabilizou as "parcerias de negócios" para "casos em que a escolha do parceiro esteja associada a suas características particulares, vinculada a oportunidades de negócio definidas e específicas, justificada a inviabilidade de procedimento competitivo".

A Norma Complementar nº 14, da Instrução Normativa nº 01/2008, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem. Dentre os tópicos, prevê que informação conforme a Lei de Acesso à Informação não pode ser armazenada na nuvem. Já informação com acesso restrito, prevista em lei, pode ser armazenada em nuvem, mas cabe ao órgão garantir a segurança.

Quanto à eventual responsabilização, a NC-14 prevê que a Alta Administração de cada órgão ou entidade é responsável pela segurança das informações tratadas em ambiente de computação em nuvem. Ademais, refere que o Gestor de Segurança da Informação e Comunicação será responsável pelas ações de implementação da gestão de risco de segurança. Expostas as normas identificadas até o presente momento, serão abordados a seguir requisitos a serem observados para viabilizar eventual contratação por órgãos públicos.

3. Critérios para contratação de *cloud service*

Salienta-se que os itens a seguir apontados não são taxativos e é provável que sejam ampliados, caso o tema seja aprofundado no futuro.

3.1. Serviço a ser contratado

Preliminarmente à contratação, necessário identificar claramente quais tipos de serviços serão contratados e quais as necessidades do órgão. Conforme identificado no Guia de Práticas para serviços de nuvem, as metas de desempenho no contexto da computação em nuvem estão relacionadas à eficiência e precisão da prestação de serviços pelo provedor de nuvem[1] (CLOUD STANDARDS CUSTOMER COUNCIL, 2015, p. 19). Ainda, o documento indica que "os clientes de nuvem devem decidir quais medidas são mais críticas para seus ambientes específicos de nuvem e garantir que essas medidas sejam incluídas em seu ANS (Acordo de Nível de Serviço)" (2015, p. 19).

[1]Medidas adicionais de qualidade do sistema que podem ser incluídas no desempenho do serviço incluem precisão, portabilidade, interoperabilidade, conformidade com padrões, confiabilidade, escalabilidade, agilidade, tolerância a falhas, facilidade de manutenção, usabilidade, durabilidade, etc.

O Acórdão n. 2569/2018-Plenário, do Tribunal de Contas da União, apresenta o resultado de uma auditoria sobre a contratação de software por organizações públicas, cuja oferta de serviço de tecnologia tem sido englobado também o *cloud service*. De acordo com o Plenário, "a computação em nuvem têm se tornado prática cada vez mais adotada pelos fabricantes, e representa um potencial risco à forma como atualmente as organizações públicas estão estruturadas para adquirir software dos fabricantes" (TCU, 2018, p. 06).

Conforme o acórdão, há três modelos de venda de software: Software como Serviço; Plataforma como Serviço e Infraestrutura como Serviço. De acordo com os modelos referidos, o TCU identifica que há dependência e vulnerabilidade significativas do Estado perante os fornecedores de tais serviços. Isso porque, além da falta de transparência e insegurança jurídica provocadas pela "complexidade dos modelos de comercialização praticados por esses fabricantes, diretamente ou por intermédio de seus revendedores" (TCU, 2018, p. 12), o software passa a ser executado na infraestrutura do fornecedor, e não do órgão adquirente (2018, p. 51).

Portanto, os modelos concedem o direito de uso do produto por determinado período, conforme as funcionalidades pré-definidas, e o planejamento prévio torna-se essencial para identificar a necessidade do órgão contratante, demonstrando vantajosidade e eficiência do objeto a ser adquirido e utilizado.

3.2. Proteção de dados

A burocracia governamental e a promoção de políticas públicas guardam relação intrínseca com a operação e tratamento de dados pessoais. Ao comparar as gerações de leis de proteção de dados no decorrer do tempo, percebe-se que a primeira geração de leis buscava proteger os dados pessoais utilizados a serviço da burocracia governamental (MENDES, 2014, p. 34). Esse cenário consolidou bancos de dados descentralizados do governo, com vistas ao aumento da eficiência das funções e finalidades estatais: previdência, tributação, saúde pública, educação, por exemplo.

Com o desenvolvimento tecnológico, o Estado percebeu as vantagens da unificação dos bancos de dados. A segunda geração volta-se à tutela da privacidade informacional, uma vez que se percebe a impossibilidade de proteção total pelo Estado dos dados disponíveis, passando a importar o consentimento do titular dos dados (DONEDA, 2006, p. 372). A terceira geração é marcada pela decisão do Tribunal Constitucional Federal Alemão de 1983, por meio da qual foi reconhecido o direito fundamental à autodeterminação informacional. Já a quarta geração busca sanar as lacunas anteriores, informando o titular de dados sobre coleta,

armazenamento e tratamento dos dados (BIONI, 2019, p. 113). Assim, percebe-se que a proteção de dados surge no contexto público, a partir da relação entre Estado e cidadãos.

No caso do serviço de nuvem, mesmo que se preveja que dados sigilosos serão mantidos no datacenter do SERPRO, sabe-se, conforme manifestação do Supremo Tribunal Federal nas Ações Diretas de Inconstitucionalidade (ADIs)[2] contra a Medida Provisória (MP) 954/2020, que não existem dados insignificantes. Atualmente, a possibilidade de cruzamento, compartilhamento, entre outros mecanismos, podem comprometer as liberdades civis e, no caso da operação e tratamento de dados por entidades privadas, a segurança nacional.

Exemplificativamente, vale mencionar o escândalo de segurança nacional nos Estados Unidos, que acusou a empresa chinesa Huawei de espionagem cibernética, o que também ocorreu em outros países, onde também sofreu embargos comerciais (THE ECONOMIST, 2019). Trata-se da mesma empresa contratada por vários órgãos brasileiros para a prestação de serviços digitais e de armazenamento de dados, dentre eles, o próprio SERPRO, que fornece formação técnica para operação dos sistemas Huawei (UNISERPRO).

Nesse ponto, o contratante deverá observar os itens que considera indispensável, ou seja, que preencha sua necessidade; e avaliar os modelos de software que se adequem aos requisitos e que garantem a proteção dos dados mediante métodos seguros, como criptografia ou outros que podem emergir ao longo do tempo.

4. Considerações finais

Buscou-se analisar as bases legais e os critérios de contratação de serviço de *cloud service* por órgãos públicos, tema ainda que deverá ser objeto de inúmeras abordagens pelos Tribunais brasileiros. Foi possível identificar a necessidade de que os contratantes procedam um planejamento prévio e contínuo de forma aprofundada em razão dos diversos modelos de serviço de nuvem ofertados no mercado, e que garantam tanto a segurança dos dados enviados ao contratado, como também sejam os mesmos protegidos em relação a terceiros. Padrões e certificações de segurança dos servidores de serviço de armazenamento em nuvem podem ser uma forma de se efetivar maior segurança na execução do contrato.

A hipótese se confirma parcialmente, ou seja, confirma-se que os órgão públicos deverão buscar proteger seus dados - principalmente se forem de segurança nacional - e os dados dos cidadãos, mas verificou-se que, após a análise preliminar do tema, considerou-se

[2] As ações foram propostas pelo Conselho Federal da Ordem dos Advogados do Brasil – OAB (ADI 6387), pelo Partido da Social Democracia Brasileira - PSDB (ADI 6388), pelo Partido Socialista Brasileiro – PSB (ADI 6389), pelo Partido Socialismo e Liberdade – PSOL (ADI 6390) e pelo Partido Comunista do Brasil (ADI 6393).

necessário seu aprofundamento em ulterior estudo, como por exemplo, em relação à possível emergência de outros critérios a serem observados em eventual contratação.

5. Referências

BENNER, Katie; CONGER, Kate. Cisco to Pay $8.6 Million to Settle Government Claims of Flawed Tech**. The New York Times**. 31/07/2019. Disponível em: https://nyti.ms/3fqXWMO. Acesso em: 14 jun. 2020.

BIONI, Bruno. **Proteção de dados pessoais:** A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

CLOUD STANDARDS CUSTOMER COUNCIL. Practical Guide to Cloud Service Agreements. version 2.0. april, 2015. Disponível em: https://bit.ly/3fnqruv. Acesso em: 13 jun. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

GOVERNO FEDERAL. **Estratégia brasileira para a transformação digital.** 2018. Disponível em: https://bit.ly/3d1SXjG. Acesso em: 13 jun. 2020.

GOVERNO FEDERAL. **Guia de Boas Práticas:** Lei Geral de Proteção de Dados (LGPD). 27/03/2020. Disponível em: https://bit.ly/2UJhqnH. Acesso em: 13 jun. 2020.

MCTIC. **MCTIC e Cisco anunciam parceria para aceleração digital do Brasil**. 27/05/2020. Disponível em: https://bit.ly/2Y4Y5zH. Acesso em: 13 jun. 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MINISTÉRIO DA ECONOMIA. **Consulta pública nº 4/2020**. Disponível em: https://bit.ly/30BBa0q. Acesso em: 14 jun. 2020.

SERPRO. **Serpro e AWS juntas para impulsionar a transformação digital do país.** Disponível em: https://bit.ly/3e28ilS. Acesso em: 13 jun. 2020.

TCU. **Acórdão 2569/2018-Plenário**. Disponível em: https://bit.ly/37s0M1f. Acesso em: 13 jun. 2020.

THE ECONOMIST. **Huawei has made a peace offering that deserves consideration.** 12/09/2019. Disponível em: https://econ.st/37sGowQ Acesso em: 14 jun. 2020.

UNISERPRO. **Configuração Huawei.** Disponível em: https://bit.ly/3hqJhCN. Acesso em: 14 jun. 2020.