II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

ADMINISTRAÇÃO PÚBLICA, MEIO AMBIENTE E TECNOLOGIA

A238
Administração Pública, Meio Ambiente e Tecnologia [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Valmir César Pozzetti; Lucas Gonçalves da Silva; Pedro Gustavo Gomes Andrade. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-273-6
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

ADMINISTRAÇÃO PÚBLICA, MEIO AMBIENTE E TECNOLOGIA

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 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 oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 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, mais uma vez, 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 pesquisa de excelência no universo da economia do conhecimento. A SKEMA 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. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

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

Belo Horizonte-MG, 09 de junho de 2021.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

COMPLIANCE DE DADOS E O USO DE TECNOLOGIAS: MITIGAÇÃO DE ATAQUES CIBERNÉTICOS INTENSIFICADOS PELO TRABALHO REMOTO DO SERVIDOR PÚBLICO

COMPLIANCE OF DATA AND THE USE OF TECHNOLOGIES: MITIGATION OF CYBER ATTACKS INTENSIFIED BY THE REMOTE WORK OF THE PUBLIC SERVER

Rhaissa Souza Proto [1]
Arthur Pinheiro Basan [2]

Resumo

A pandemia causada pelo coronavírus acelerou o processo de avanços tecnológicos, acarretando maior circulação de dados pessoais. Dentre as medidas impostas para combate à pandemia destaca-se o isolamento social que, consequentemente, aumentou significativamente os números de servidores em regime de trabalho remoto. O objetivo deste estudo, que não se pretende ser exauriente, é abordar quais as medidas necessárias, no âmbito da Administração Pública, para tomada de atitudes para segurança de dados de terceiros expostos, já que, com a expansão do uso de computadores alheios à rede da Organização houve aumento de ataques cibernéticos que podem comprometer todo o sistema público.

Palavras-chave: Compliance, Dados, Cibernético, Tecnologias, Administração

Abstract/Resumen/Résumé

The pandemic caused by coronavirus accelerated the process of technological advances, leading to greater circulation of personal data. Among the measures imposed to combat this, social isolation stands out, consequently, significantly increased the number of civil servants in remote work regime. The objective of this study, which isn't intended to be exhaustive, is to address what measures're necessary, within the scope of Public Administration, to take attitudes towards data security of exposed third parties, with the expansion of the use computers outside the network of the Organization there was increase in cyber attacks that can compromise the entire public system

Keywords/Palabras-claves/Mots-clés: Compliance, Data, Cybernetic, Technologies, Management

[1] Mestranda profissional em Direito da Empresa e dos Negócios- UNISINOS. Especialista em direito do Trabalho -EDH. Graduada em Direito- UniRV. Coordenadora de Delimitação e Análise da FUNAI. Contato eletrônico: rhaissaproto@hotmail.com

[2] Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Mestre em Direito pela Universidade Federal de Uberlândia – UFU. Professor adjunto na UniRV. Contato eletrônico: arthurbasan@hotmail.com

1 INTRODUÇÃO

É inegável que a pandemia causada em decorrência da infecção humana pelo coronavírus (Sars-Cov-2), popularmente designado como novo coronavírus, trouxe reflexos transversais para o cotidiano, para a ciência do direito, bem como impulsionou diversos avanços tecnológicos. Nesta seara, como o distanciamento físico se trata de uma das medidas impostas para contenção da disseminação do vírus, abordando aqui especificamente dos servidores públicos, inúmeros destes passaram a exercer seus ofícios em modo de trabalho remoto. Decorrente desse novo momento desafiador e com ele um novo modo de se conduzir o trabalho no Âmbito da Administração Pública, surgiram diversos imbróglios, alguns apontados para reflexão no presente texto.

Neste momento pandêmico, com o aumento da utilização da internet, a exposição de dados se destacou, tornando-se um assunto de grande relevância social. Tanto é que, em meio a corrida para combate da pandemia causada pelo coronavírus, a Lei Geral de Proteção e Dados Pessoais brasileira (Lei nº 13.709/18, a LGPD) entrou em vigor no dia 18 de setembro de 2020 (BRASIL, 2018), sendo mencionada expressamente ainda antes em julgamentos no STF.[1] No âmbito das organizações públicas e privadas houve um recrudescimento dos ataques cibernéticos, sendo uma das causas dessa ocorrência a necessidade de trabalho remoto pelos servidores e o uso por seus computadores particulares.

Pois bem, frente à relevância do tema para a sociedade e ressaltando que mesmo após o fim do cenário pandêmico o trabalho remoto será uma realidade para os servidores de uma organização, parte-se da seguinte problemática: através de quais mecanismos a Administração Pública poderá garantir a segurança dos dados das informações dispostas diante dos ataques cibernéticos?

No afã de que o presente estudo alcance sua finalidade, o objetivo geral do texto será apresentar a necessidade de aplicação de um programa de *compliance* de dados na organização que, com o auxílio da utilização de novas tecnologias, podem garantir a segurança dos dados de terceiros

[1] Em maio de 2020, no julgamento das cinco Ações Diretas de Inconstitucionalidade contra a Medida Provisória 954/2020, que previa o compartilhamento de dados de usuários por prestadoras de serviços de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), o STF reconheceu a proteção de dados direito como fundamental. Ações ajuizadas pelo Conselho Federal da Ordem dos Advogados do Brasil (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). BRASIL. Supremo Tribunal Federal. ADI 6387 - Ação direta de inconstitucionalidade. Requerente: Conselho Federal da Ordem dos Advogados do Brasil – CFOAB. Intimado: Presidente da República Relator: Min. Rosa Weber. Brasília, DF, 7 de maio de 2020. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 05 maio 2021.

disponíveis aos servidores que ao realizarem o labor de seus computadores particulares. Isso porque, por haver a possibilidade de não estarem estes em conformidade com a política de segurança da organização que pertencem, estão susceptíveis a ataques cibernéticos podendo comprometer toda a Administração. Nessa senda, serão expostos assuntos sobre o imbróglio do tema levado a efeito neste trabalho.

Almeja-se com o presente estudo demonstrar que a inserção de tecnologias específicas, através da implementação do *compliance* de dados, é a maneira eficaz para mitigar os ataques cibernéticos. Isso porque, com o aumento de servidores em trabalho remoto, o risco de vazamento de dados de terceiros sensíveis pode trazer inúmeros danos à Administração Pública, que em alguns casos podem ser irreversíveis.

2 COMPLIANCE DE DADOS: COLETA E TRATAMENTO DE DADOS NO ÂMBITO PÚBLICO DIANTE DO AUMENTO DO CONTINGENTE DE SERVIDORES EM TRABALHO REMOTO

Com o advento da LGPD a tendência à governança ganhou novos contornos. Paulatinamente, assevera Faleiros Júnior (2020, p. 122) que diversas modificações sociais passaram a afetar a inovação e oportunizaram o surgimento de novas tecnologias, acirrando riscos já existentes e surgindo novos, conduzindo ao fato de que a mera existência da norma não garante a proteção e contingenciamento a todas as individualidades envolvidas na efetiva proteção à pessoa.

Explica Saavedra (2021, p.731) que uma das grandes novidades que as legislações recentes sobre proteção de dados trouxeram foi o perfilhamento da sistemática de *compliance* como método interno de conexão entre os vários institutos do direito, acrescentando que o sistema de gestão de *compliance* de dados aparece como locução do princípio da *accountability* e como meio de vigilância para garantir proteção dos dados. Enfatiza-se, neste ponto, que em face do recrudescimento dos ataques cibernéticos as organizações públicas e privadas, tem a necessidade de observação de normas de segurança da informação exarada por aquele órgão. A administração Pública deve atendimento à referida base de dados que se encontram compiladas no sítio eletrônico do governo federal do Brasil[2]. A observância desse pacote foi enfatizada pelo Tribunal de Contas da União nos Acórdãos nº 1233/2012 (BRASIL, 2021) e nº 3051/2014–TCU – Plenário (BRASIL, 2014).

2 https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao

Em um outro viés, na perspectiva de Faleiros Júnior (2020 p.124), é cediço que o *big data* público já é uma realidade no nosso cotidiano, passando assim o controle de dados exercido pelo Poder Público a assumir uma nova dimensão com a possibilidade de compartilhamento interorgânico.

Esses dados em comento integram-se os tão notórios *big datas*, que na perspectiva de Gonzáles (2016, p. 17) referem-se a "[...] grandes quantidades e informação digital controlada por companhias, autoridades e outras organizações, sujeitas a uma análise extensa baseada em algoritmos". A utilização dos dados, por si só, não consegue causar esfacelos, com exceção de aplicação por terceiros sem o consentimento do manuseio das personalidades a eles interligados. Nesse sentido, Faleiros Júnior (2020, p. 289) traz a conceituação de *big data* como sendo:

> "[...] nada mais é que um enorme banco de dados no qual se armazena todo tipo de informação para que, posteriormente, se trabalhe com esses bancos de dados, cruzando as informações coletadas através de algoritmos, oferecendo possibilidades variadas de previsão de eventos futuros e, ainda, condições de se identificar correlação de dados a partir de causalidades complexas, oferece possibilidades de análises estatísticas infindáveis, normalmente se valendo de amostragens. Quanto maior o banco de dados, maior é a sua confiabilidade e, consequentemente, mais precisa será a aferição obtida pelo algoritmo utilizado na testagem proposta."

O crescimento do número e da diversificação dos dados que podem ser combinados teve uma evolução rápida especialmente pelo uso intensivo da Internet (destacando-se, ainda mais o período pandêmico em que o distanciamento físico elevou o número de usuários da web), ilimitado no espaço e no tempo, elevando o risco de re-identificação mesmo após a anonimização de bases isoladas (MOONEY e PEJAVER, 2018). Destaca-se ainda o fato de que os mercados que são ricos em dados e cercados por segredos quanto a aplicação de seus algoritmos, os quais são utilizados para propiciar uma vantagem concorrencial e os danos decorrentes dessa obscuridade são variados (FALEIROS JÚNIOR, 2020). Frank Pasquale (2015) define esse quesito como caixas-pretas (*black boxes*).

Os dados atualmente são considerados o novo petróleo, conforme argumenta Flender (2019, np) frase originalmente em inglês "*data is the new oil"*, inspiração do especialista em ciência de dados Clive Humby, reflete o quanto são inesgotáveis e expansíveis. Nesse sentido, demonstra-se a importância de empresas que lidam com dados pessoais aplicarem programas de *compliance*. A LGPD é trabalhada estimulando a autorregulação, o que se reflete na verdade numa co-regulação, auxiliada pela tecnologia. Importante entender que a tecnologia pode ser um importantíssimo vetor ou mecanismo regulatório, que no caso da proteção de dados tem um

grande potencial para ser utilizado, e que quanto mais se atentar para as probabilidades de risco, menor a chances de vazamento de dados, enfatizando, *in casu*, no âmbito da Administração Pública.

Com efeito, partindo da maior incidência dos servidores em trabalho remoto aumenta-se o fluxo de informações pela rede, frente ao acréscimo do número de estações de trabalho, pela adoção do Sistema Eletrônico de Informações a nível nacional e alocação constante de novos recursos computacionais na infraestrutura da Organização. Diante disso, possíveis ataques cibernéticos demandam maior vigilância dos dados. Nesses casos, elucida Silva (2003, p. 112-113) que por ser utilizado sistemas e plataformas digitais que envolvem a colheita, tratamento ou armazenagem de dados, ou possivelmente o compartilhamento de tecnologias, implicarão a necessária observância a tais parâmetros. Diante dessa viabilidade, necessário discutir-se sobre a implementação de tecnologias para efetivação do programa de *compliance* de dados.

3 IMPLEMENTAÇÃO DE TECNOLOGIAS QUE VISEM MITIGAR ATAQUES CIBERNÉTICOS: O COMPLIANCE DE DADOS

A partir do momento que o servidor laborando em trabalho remoto, utiliza o seu computador particular para acessar sistemas, e-mails ou qualquer outro meio para ingresso às plataformas que contenham dados disponíveis à ele para realização do ofício, é imprescindível que a Organização tenha meios para garantir o impedimento de ataques cibernéticos. Já que, se incorrer nesse acometimento, pode haver danos e prejuízos em larga escala para toda a Administração Pública que possui inúmeros dados sensíveis de terceiros.

Sobre esse ponto, quando já acometido com o problema, os responsáveis pela administração do servidor invadido deverão realizar levantamento de vulnerabilidades para adotar medidas cabíveis ao fortalecimento e aprimoramento dos níveis de segurança do ambiente institucional. Referida ação reduzirá a capilaridade das vulnerabilidades a serem exploradas, diminuindo assim as possibilidades de ocorrências semelhantes no futuro.

Neste interregno, a utilização do *compliance* de dados através do uso de tecnologias será o meio eficaz para atuação nesse ponto. O setor de Tecnologia de Informação e Comunicação (TIC) de uma organização é o principal aliado para implementação desses mecanismos. Destaca-se, ainda, que os usuários das contas de TIC são os que mais necessitam de fortalecimento dos padrões de segurança.

O uso de tecnologias é um grande auxiliar para implementação em rotina de ação como meio de enrijecimento das estruturas de segurança e política de acesso, já que com registro de eventos

de ataques cibernéticos ligados ao usuário do servidor, propicia-se o início imediato de atividades de identificação e qualificação destes e após a caracterização, comunica-se junto a equipe técnica especializada para solução do caso e visando evitar demais ataques.

A aplicação do *compliance* de dados encarregar-se-á de realizar o levantamento de vulnerabilidade que viabiliza aos administradores dos servidores, adotando medidas cabíveis de mitigação do risco e de fortalecimento e aprimoramento dos níveis de segurança do ambiente organizacional. Com essa diminuição, abranda-se a possibilidade de ocorrências futuras.

Dentre os mecanismos que se pode utilizar, é válido destacar os seguintes: bloqueio de conta após 3 (três) tentativas de acesso com credenciais inválidas; adequação dos privilégios das Políticas de grupo de domínio, em especial aquelas referentes a ações sensíveis como alterar horário do sistema, desligar sistema, forçar o desligamento a partir de um sistema remoto e permitir *logon* local; diferentes configurações dessas políticas para os diferentes tipos de servidores (destacando que os pertencentes ao TIC necessitam de ainda mais vigilância).

Essas ações aumentam os níveis de proteção do ambiente da Organização tornando-as menos susceptíveis a ataques cibernéticos que logrem êxito, garantindo assim, a segurança de dados de terceiros. Referidas condutas, através do *compliance* de dados, reforçam o caráter protetivo às informações geradas e geridas pela Administração, protegendo, consequentemente, as credenciais de acesso de seus usuários e dificultando o acesso indevido a informações por meio de *logins* comprometidos.

Adentrando ao ponto de que o servidor em trabalho remoto tem em seu poder dados, na maioria das vezes sensíveis, de terceiros, a regra a ser aplicada é a mesma para o trabalho físico. Isso porque o que irá conscientizá-lo e demonstrar os riscos advindos do compartilhamento, tanto de forma individual como globalizada, se trata da disseminação da cultura de *compliance*.

Para essa ocorrência, a Alta Administração é a válvula motriz para a dissipação. Com a utilização efetiva do Programa de *Compliance*, os administradores resguardam a si e a todos (GAZONI, 2019, p. 88). Para melhor compreensão o Guia de Programa de Integridade para Empresas Privadas, da Controladoria Geral da União (BRASIL, 2015, p.8) elucida que:

> O comprometimento da alta direção da empresa com a integridade nas relações público-privadas e, consequentemente, com o Programa de Integridade é a base para a criação de uma cultura organizacional em que funcionários e terceiros efetivamente prezem por uma conduta ética. Possui pouco ou nenhum valor prático um Programa que não seja respaldado pela alta direção. A falta de compromisso da alta direção resulta no descompromisso dos demais funcionários, fazendo o Programa de Integridade existir apenas "no papel".

Nesse ínterim, a Organização pode se valer de inúmeras ações. Valendo-se do ponto que o presente estudo objetiva buscar meios para segurança de dados de terceiros em poder dos servidores que se encontram em trabalho remoto, uma das medidas a serem tomadas é a disponibilização de uma série de vídeos pelo departamento de TIC, os quais podem ser disponibilizados em canais institucionais e, a fim de ter uma relação aproximada, bem como conhecer as dificuldades enfrentadas pelo servidor, permitir a interação ao final entre os participantes. Esses vídeos podem apresentar conceitos básicos da segurança da Informação, demonstrar as principais ameaças e ataques cibernéticos, a privacidade na internet, como cuidar dos dados na Organização, utilização de aplicativos e tecnologias como estratégia para melhorar sua segurança.

Pelo exposto, de forma a atender de maneira satisfatória aos requisitos técnicos de segurança difundido na área de proteção de dados, principalmente com grande parcela de servidores em escala de regime de trabalho remoto, faz-se necessário investimento para aquisição de equipamento de alta performance para proteção do perímetro de rede da Organização. Tal contratação é um mecanismo eficaz na implementação do *compliance* de dados na área pública, já que terá por meta a melhorias na descoberta, identificação e mitigação de incidentes de segurança de rede.

4 CONCLUSÃO

O desafio nesse momento é detectar quais seriam as melhores estratégias para se tomar diante do elevado número de aumento de servidores em trabalho remoto, uma vez que, após a ocorrência de incidentes pelo uso de dados ocorrer de forma equivocada ou indesejada, os eventuais danos financeiros, as penalidades e os danos reputacionais podem gerar incalculáveis impactos para a Administração Pública.

Em síntese, com maior compartilhamento de informações significa maior risco de vazamentos, o que exsurge a necessidade de uma maior vigilância e aprimoramento da segurança dos dados. A razão para isso decorre do invariável tráfego informacional que surge do uso de qualquer tecnologia aplicada ao exercício da gestão pública, enfatizando o aumento diante da quantidade de servidores alocados em regime de teletrabalho. Na medida em que o tratamento de dados incita riscos, o *compliance* de dados surge como solução para a mitigação destes e a fim de que se tenha o devido respeito à transparência em todos os seus níveis.

REFERÊNCIAS

BRASIL. **Lei nº. 13.709**, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/Lei/L13709.htm>. Acesso em: 04 de maio de 2021.

BRASIL. Tribunal de Contas da União. Acórdão nº 1233/2012 – TCU – Plenário 1. Processo nº TC 011.772/2010-7. Relator: Ministro Aroldo Cedraz. Disponível em < http://www.ifam.edu.br/portal/images/file/0000029368-Acord+%C3%BAo%201233_2012_TCU-Plenario.pdf>. Acesso em 06 de maio de 2021.

BRASIL. Tribunal de Contas da União. Acórdão nº 3051/2014 – TCU – Plenário. Processo nº TC 023.050/2013-6. Relator: Ministro-Substituto Weder de Oliveira. Disponível em < https://www.cjf.jus.br/publico/biblioteca/Acord%C3%A3o%2030512014.pdf>. Acesso em 05 de maio de 2021.

CONTROLADORIA GERAL DA UNIÃO (CGU). **Programa de Integridade - Diretrizes para empresas privadas**. Setembro, 2015. Disponível em: <https://www.legiscompliance.com.br/images/pdf/programa_integridade_diretrizes_para_empresas_privadas_cgu.pdf>. Acesso em 03 de maio de 2021.

FLENDER. Samuel. *Data is not the new oil*. 10 de fevereiro de 2019. Disponível em <https://towardsdatascience.com/data-is-not-the-new-oil-bdb31f61bc2d>. Acesso em 05 de maio de 2021.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração pública digital:** proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. São Paulo: Editora Foco, 2020.

GONZÁLEZ, Elena Gil. ***Big data, privacidade y protección de dados***. Madris: Agencia Española de Protección de Datos. 2016. Disponível em: < https://www.researchgate.net/publication/324831404_Big_data_privacidad_y_proteccion_de_datos>. Acesso em: 27 set. 2020.

KALAY, El Marcio, CUNHA, Matheus – Organizadores, GAZONI, Carolina - Capítulo 4 - **Manual de Compliance – Compliance Mastermind** Vol. 1 – LEC – Legal Ethics Compliance.

MOONEY, S. J.; PEJAVER V. Big data in public health: terminology, machine learning, and privacy. **Annu Rev. Public Health,** 2018, nª 39, p.95-112.

PASQUALE, Frank. **The black box society:** Cambridge: Harvard University Press, 2015. Disponível em **<**https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf>. Acesso em 11 set 2020.

SAAVEDRA, Giovani Agostini. **Compliance na área da saúde**. São Paulo: Lykoscastle, 2016.

SILVA. Miguel Moura e. **Inovação transferência de tecnologia e concorrência: estudo comparado do direito da concorrência dos Estados Unidos e da União Européia**. Coimbra: Almedina, 2003, p. 112-113