Journal of Technology & Information

Os Três Pilares da Segurança da Informação na Internet Chinesa

The Three Pillars of Information Security in Chinese Internet

Recebido: 22/06/2022 | Revisado: 30/06/2022 | Aceito: 30/06/2022 | Publicado: 30/06/2022
https://www.doi.org/10.5281/zenodo.6794524

Karlla Soares Couto
FATEC Santana de Parnaíba
https://orcid.org/0000-0001-9973-2663
karllasoares713@gmail.com

Yara Rodrigues Amorim
FATEC Santana de Parnaíba
https://orcid.org/0000-0003-4950-9580
yaramorim06@gmail.com

Karoline Macedo de Lima
FATEC Santana de Parnaíba
https://orcid.org/0000-0002-4962-2148
karolinemacedo.lima@gmail.com

Irapuan Glória Júnior
Fatec Santana de Parnaíba
https://orcid.org/0000-0003-2973-3470
ijunior@ndsgn.com.br

Resumo

Há setenta anos a República Popular Chinesa vivência o resultado de uma revolução social, os impactos desta são observados em diversas áreas, incluindo os campos da tecnologia da informação. Os recentes conflitos políticos que os chineses vêm presenciando têm sido um dos motivos de a internet no país estar cada vez mais restrita ao contato com o resto da rede mundial de computadores, o que impacta diretamente na cultura e economia local. Desta forma, este estudo visa comparar os conceitos de confidencialidade, integridade e disponibilidade com a atual conjuntura virtual chinesa, utilizando revisão sistemática para a análise de artigos sobre o tema. Evidenciando as limitações impostas pelo governo e os desafios impostos para os gestores que desejam empreender no país.

Palavras-Chave: China, Redes, Disponibilidade, Confidencialidade, Integridade, Segurança da Informação.

Journal of Technology & Information

Abstract

For seventy years, the People's Republic of China has been experiencing the result of a social revolution, the impacts of which are observed in several areas, including the fields of information technology. The recent political conflicts that the Chinese have been witnessing have been one of the reasons why the internet in the country is increasingly restricted to contact with the rest of the world wide web, which has a direct impact on the local culture and economy. Thus, this study aims to compare the concepts of confidentiality, integrity and availability with the current Chinese virtual environment, using a systematic review to analyze articles on the subject. Evidencing the limitations imposed by the government and the challenges imposed for managers who wish to undertake in the country.

Keywords**:** China, Networks, Availability, Confidentiality, Integrity, Information Security.

1. Introdução

A China alcançou a marca de mais de 1 bilhão de usuários na internet (CCNIC, 2021), resultado do avanço da tecnologia e a informatização das cidades com tecnologia baseadas em Internet das Coisas (IoT), aliada à soluções de alta qualidade em tecnologia e o aumento das preocupações com a privacidade dos dados acumulados para seu funcionamento aumentam de forma exponencial (Yang & Xu, 2018).

O início do uso da internet fora de forma comercial no país, o governo local demonstra profundo interesse na regulação do uso da rede mundial de computadores, e realizou várias propostas de regulamentação internacional em conferências (Cheung, 2018). O Estado chinês tem poder de influenciar o consumo, coleta e análise de dados em contextos de mídias sociais e *BigData* (Jiang & Fu, 2018).

Diante deste contexto, este estudo pretendeu responder alguns questionamentos criados: como o país incorpora em suas políticas regulamentárias para o mundo virtual os conceitos de Confidencialidade/*Confidentiality*, Integridade/*Integrity* e Disponibilidade/*Availability*, conhecidos como a tríade CIA da segurança da informação? Como a legislação chinesa regula a internet? E quais influências estatais podem ser observadas? A pretensão desta pesquisa não é debater a ética sobre o controle de dados

pelo governo chinês, mas trazer uma análise sobre o tratamento das informações em termos de segurança da informação.

2. Referencial Teórico

2.1. Pilares da Segurança da Informação

Os princípios mais importantes no desenvolvimento de aplicações seguras são retratados pelo triângulo CIA (Hintzbergen et al., 2018), que contém os conceitos de confidencialidade, integridade e disponibilidade dos dados relativos a toda instalação de software, análise de dados ou fornecimento de acesso a algum dado ou outra informação (Tipton et al., 2016).

O triângulo CIA é citado na norma ISO 27001 ao especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente qualquer sistema de gerenciamento de segurança da informação (ISO, 2013). Ainda segundo a norma, os princípios são definidos como: (1) Confidencialidade/*Confidentiality*; (2) Integridade/ *Integrity*; e (3) Disponibilidade/*Availability*.

A **confidencialidade**, pode ser chamada também de exclusividade, trata dos limites determinados de acessos a uma informação, por exemplo, uma pessoa em determinado cargo não possui interesse organizacional em documentos de um outro departamento e deve sofrer medidas protetivas aos dados como criptografias, autenticação, *traffic padding, etc* (Hintzbergen et al., 2018).

A ISO define como a garantia de que uma informação só seja acessada por indivíduos autorizados, por meio de autenticação, que é a medida de confidencialidade mais utilizada, pois garante que a pessoa que utiliza um serviço está no controle sobre um ou mais acessos associados àquela identidade virtual (Grassi et al., 2017).

Em relação a **integralidade**, corresponde a prática do conceito de garantir que uma informação continue completa e exatamente da forma que deveria estar (Fernandes, 2013), e que qualquer modificação não autorizada de dados, quer tenha sido realizada deliberadamente ou acidentalmente, incorre em uma violação da integridade dos dados (Hintzbergen et al., 2018). Assim, a integridade se refere a manter a informação no estado desejado por seus administradores, mesmo que esteja incorreta.

A **disponibilidade** visa garantir que a informação esteja disponível para o usuário com autorização que necessitar acessá-la, porém, deve ser avaliada e direcionada aos usuários de acordo com as políticas da organização e do país, e nem sempre são restringidas por questões de segurança da informação (Diana et al., 2016).

A organização chinesa GreatFire.org possui a ferramenta *GreatFire Analyser* que monitora os sites bloqueados para acesso ao público comum pelo governo chinês. Segundo eles, desde 2011 a China tem bloqueado inúmeros sites com domínios da empresa Google, que são informados no Website. O site https://www.google.com/ não foi bloqueado, sendo apenas uma ferramenta de pesquisa (GREATFIRE, 2011).

2.2. Contexto Socioeconômico Chinês

A república popular da China foi declarada em 1949, com sua reorganização de moldes apoiados pela então união soviética (Guillermaz, 1968). A partir de 1958 a china aplica seu segundo plano quinquenal, plano este que tinha a pretensão de transformar o país em um território desenvolvido em tempo recorde, o que acabou sendo um grande fracasso levando Mao a ser afastado da direção da república (Pomar, 2003).

Na conhecida “Era Pós Mao” foram adotadas as quatro modernizações, iniciando a abertura econômica do país para o capitalismo, criando o Socialismo de Mercado, o que permite a china receber investimentos privados e estrangeiros, por meio das Zonas Econômicas Especiais (Pomar, 2003). O comércio exterior somente começa a se tornar peça-chave para o crescimento da economia chinesa no final da década de 1980, quando tanto exportações quanto importações ultrapassam 15% do PIB (Nonnenberg, 2010).

A Conferência Nacional da Ciência em 1978, tinha como objetivo apresentar publicamente o apoio do governo a ciência e tecnologia. O projeto de Oito Anos apresentado na conferência, teve um apelo para um aumento de pesquisadores para assim alcançarem níveis internacionais e a inserção em campos como ciência a laser, física de alta energia e voos tripulados ainda em meados dos anos 80 (Cao et al., 2006).

Segundo o estatuto da Academia Chinesa de Ciências, denominado em chinês tradicional:中国科学院院士, foi criada em 1992, seus membros devem promover a ciência e tecnologia, desenvolverem uma força de trabalho cientifica, defenderem e manterem seu espírito científico, participarem de reuniões de membros, promoverem intercâmbios e receberem tarefas de consulta e avaliação (CAS, 1996).

2.3. Interferência Política Na Internet

A República Popular Chinesa possuía mais de 800 milhões de pessoas conectadas à internet em 2018 (CCNIC, 2021). Apesar de liderar o ranking de países com maior número de pessoas conectadas a internet desde 2008, a conexão ainda está à sob o, popularmente mencionado, Grande Firewall da China. Em território chinês a segurança do espaço virtual é vista como uma extensão das funções do governo (Miao et al., 2018).

A internet chegou oficialmente em território chinês em 1994, por meio do projeto Ponte Dourada. Conforme crescia era observada com inquietude pelo governo, o que culminou no projeto Escudo Dourado, que começou a ser implementado em 1996, pelo Ministério da Segurança Pública Nacional. Neste mesmo ano é decretado que qualquer acesso a plataformas digitais deverá ser através de linhas de comunicação internacionais controladas pelo Ministério dos Correios e Telecomunicações (Jiang & Fu, 2018).

Na época, os equipamentos Cisco continham controladores de acesso para monitorar os usuários e negar acesso a conteúdo considerado inapropriado. Utilizado de base para o início da censura, a *blocklist* chinesa inicialmente contava com mais de cem sites bloqueados como constatado pela primeira vez num estudo acadêmico (Zittrain & Edelman, 2003). Posteriormente, a censura começou a abranger sites políticos, religiosos, de diretos humanos e que promoviam "valores ocidentais".

A Administração do Ciberespaço da China (CAC) é responsável por administrar e controlar os conteúdos presentes na rede chinesa, é o órgão governamental que atua no bloqueio de palavras, produtos e IP's (Creemers, 2016). Conforme a lista divulgada pelo Xinhua, entre os sites proibidos, estão os mais acessados do ocidente, como os serviços *Whatsapp, Twitter, Instagram, Facebook, Dropbox, Tumblr e Pinterest*.

A china possui versões análogas aos sites banidos, como o Sina Weibo, que mescla as funcionalidades do Facebook e Twitter. Em aplicações como esta, onde é possível utilizar um *nickname,* é necessário um registro do nome oficial, para que o governo tenha o controle dos usuários para fins de identificação e possíveis acionamentos judiciais. Também é utilizado um sistema de pontuação do comportamento individual online, que resultavam em restrições para indivíduos com conduta considerada prejudicial (Creemers, 2016).

3. Metodologia

O presente estudo desenvolve uma revisão sistemática baseada nas diretrizes de Kitchenham (2008), com o objetivo de apurar pesquisas sobre o uso da internet na China e suas restrições, e a coleta de dados via documentos digitais. A metodologia de Kitchenham permite a realização de uma pesquisa com mais precisão de informações e objetividade ao responder às questões de pesquisa. A pesquisa será de natureza qualitativa e baseada em artigos científicos, conforme Tabela 1.

Tabela 1 - Características da pesquisa

Item	Conteúdo	Autores
QP 1	Como os pilares da segurança da informação (confidencialidade, integridade e disponibilidade) são aplicados na política virtual chinesa?	
QP 2	Quais são as legislações relacionadas à internet da China?	
QP 3	Como a influência governamental afeta a internet no país?	
Natureza	Qualitativa	Martins & Theodoro (2009)
Metodologia	Revisão sistemática	Kitchenham (2008)
Coleta de dados	Artigos científicos	
Unidade de Análise	Área de tecnologia da informação no país	

3.1. Questões de Pesquisa

As questões de pesquisas pelo estudo são:

- QP1: Como os pilares da segurança da informação (confidencialidade, integridade e disponibilidade) são aplicados na política virtual chinesa?
- QP2: Quais são as legislações relacionadas à internet da China?
- QP3: Como a influência governamental afeta a internet no país?

3.2. Processo de Pesquisa

Os artigos foram pesquisados pelo *Google Scholar* com as palavras-chave "China", "Segurança" e "Internet". A pesquisa resultou em um total de 13 artigos candidatos e 8 artigos selecionados.

3.3. String

A *string* a ser aplicada no *Google Sc*holar é:

((“China”) AND (“Segurança” OR “Security” OR “Cybersecurity”) AND (“Internet” OR “WWW” OR “Digital”)) OR ((“China”) AND (“Segurança” OR “Security” OR “Cybersecurity”) AND (“Internet” OR “WWW” OR “Digital”) AND (“Confidentiality” OR “Integrity” OR “Availability”))

3.4. Critérios de Seleção

Os critérios para seleção foram:

- Estudos preferencialmente publicados a partir de 2016;
- Conter as palavras chaves em sua composição;
- Utilizar apenas artigos publicados e desconsiderar monografias, livros, teses e dissertações; e
- Uso de artigos nos idiomas inglês e português.

3.5. Resultados da Busca

A aplicação dos critérios resultou na Tabela 2 em que foram apresentados a quantidade de artigos resultantes da busca, denominado candidatos, e aqueles que foram selecionados em que a análise resultante da verificação se o contexto do artigo tinha relação com o tema proposto nessa pesquisa tinha sido abordado, sendo que nos anos em que não houveram candidatos e selecionados foram retirados.

Tabela 2 - Artigos Candidatos/Selecionados

Base	2003	2011	2012	2015	2016	2018	2020	Total
Google Scholar	01/01	01/00	01/00	01/00	02/01	06/05	01/01	13/05

4. Análise e Interpretação dos Resultados

4.1. Restrição de Uso na Internet Chinesa e Suas Implicações

Apresentado por 3 dos autores selecionados, são citadas interferências governamentais referentes a publicações de conteúdo. No mesmo raciocínio, 4 citam a disponibilidade parcial de certos sites (ou sua indisponibilidade).

Dentre os 4 que citam o bloqueio total ou parcial de certos sites, Zittrain e Edelman (2003) apresentam que, na época, com testes baseados em endereço IP, DNS, endereço IP do servidor, palavras-chave e redirecionamento de DNS, cerca de 18.931 sites estavam inacessíveis via rede chinesa (dentre os 204.012 utilizados para a pesquisa). Gerando também uma testagem de conteúdo sexualmente explicito, das 752 páginas listadas no google, 101 estavam indisponíveis.

O monitoramento de publicações na rede é mencionado pelo *China's Social Credit System(s)*, o sistema de pontuação dos cidadãos por boa conduta online é apresentado por dois autores distintos. Desde 2014, com a aprovação da resolução sobre violação online de direitos da personalidade, as empresas (cujo operam virtualmente) possuem a obrigatoriedade de fornecerem a tribunais dados como endereços, nomes e formas de contato de usuários acusados de publicarem informações difamatórias, colocando em dúvida a confidencialidade dos dados acumulados.

4.2. Relação com a Tríade CIA na Segurança da Informação

Desde 2003, é observado que a disponibilidade dos dados tem interferência pelo estado chinês, e um dos autores selecionados cita a indisponibilidades de sites integral ou parcialmente. Também de acordo com uma das referências, foi observado o bloqueio de palavras ou tópicos.

Nos campos da privacidade e confidencialidade, existe a centralização do tratamento dos dados pelo governo, monitorando as atividades online nas mais diversas plataformas e gerenciando quais conteúdos são passíveis de acesso, publicação e compartilhamento. É mencionado por três autores o controle governamental sobre os dados publicados, visto que a CSL define a proteção de dados como direito de todo cidadão.

É firmada a obrigatoriedade de fornecedores de serviços virtuais o compartilhamento de dados com o governo, tal qual a moderação primária dos ambientes para que não haja inconformidade legal.

Conforme pontuado em duas das referências bibliográficas, é necessária a vinculação das contas a informações de identificação da pessoa física, garantindo a integridade e o não repúdio das informações publicadas. Baseando-se nestes dados, existem programas como o *China's Social Credit System(s)*, que cria benefícios ou restrições para o usuário com base em seu comportamento na esfera virtual.

4.3. Aplicação dos Pilares da Segurança da Informação na Política Virtual Chinesa

Dentre os 8 artigos selecionados, nenhum deles cita especificamente a aplicação das políticas chinesa relacionadas aos princípios da segurança da informação baseada na tríade CIA (ISO, 2013).

A partir dessas definições da Tríade CIA, foi verificado que os artigos continham informações sobre a tratativa do governo chinês que estivessem relacionados às suas concepções (Tabela 3).

.

Tabela 3 - Artigos informando uso da tríade CIA na China, sendo (C) Confidencialidade, (I) Integridade e (A) Disponibilidade

#	Artigo	Autores	Conceitos informados		
			C	I	A
A01	A China e a política internacional das Tecnologias de Informação e Comunicação	Majerowicz (2020)	x	-	-
A02	A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services	Zhang, Tang & Jayakar (2018)	x	-	-
A03	Chinese social media and Big Data: Big Data, Big Brother, Big Profit?	Jiang & Fu (2018)	x	x	x
A04	Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century	Creemers (2016)	x	-	x
A05	Internet Filtering in China (2003)	Zittrain & Eldermain (2003)	-	-	x
A06	Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law (2018)	Yang & Xu (2018)	x	-	-
A07	The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities	Cheung (2018)	x	-	-
A08	Who's in charge of regulating the Internet in China: The history and evolution of China's Internet regulatory agencies	Miao, Zhu & Chen (2018)	x	-	-

Em relação a serviços de e-business, as corporações não devem coletar dados não autorizados ou não relacionados a usos comerciais e não devem divulgar ou vender os dados dos clientes. Porém, ao mesmo tempo que a CSL atribui obrigações de controle de dados às empresas, não informa claramente qual a obrigação do governo em relação a proteção dos dados (Yang & Xu, 2018), apesar das políticas de incentivo à segurança das informações, há outros artigos citam o chamado *China's Credit System*.

Outros dois estudos citam políticas de segurança chinesas como as Opiniões para Fortalecimento do Trabalho de Garantia de Segurança da Informação, que propunha o estabelecimento de um esquema de proteção em vários níveis, certificação obrigatória, recuperação de desastres, gerenciamento de incidentes, segurança dos aplicativos governamentais, redes confiáveis, padrões de segurança da informação e um plano quinquenal de segurança da informação (Cheung, 2018); e a Administração de Ciberespaço da China (CAC) como a instituição central chinesa a cuidar da segurança cibernética (Miao et al., 2018).

Em relação à **integridade**, apenas um dos artigos apresentou informações sobre políticas chinesas relacionadas ao conceito, afirmando que o estado chinês impõe limites ao discurso político e que se deve ser cauteloso ao coletar dados advindos da China devido a manipulação e gestão sobre a Internet (Jiang & Fu, 2018).

Foram encontrados três artigos citando políticas de **disponibilidade** em que é informado que o governo coloca barreiras nas demonstrações políticas, por mais que em 2014 um estudo encontrou muitas manifestações políticas no site Weibo, mesmo que dentro do espectro político do estado (Jiang & Fu, 2018).

Em um teste de filtragem de sites na China, um dos estudos encontrou cerca de 18 mil sites inacessíveis em dois servidores proxies, de um total de mais de 204 mil sites testados (Zittrain & Edelman, 2003).

O último informa que após as relações de Snowden em 2014 e de um artigo da Red Flag Manuscripts revelar uma série de drones próximos a costa chines movidos a energia solar, que forneciam Internet via wi-fi sem conhecimento do governo chinês, a política de barramento de conteúdo e equipamento estrangeiro iniciou, conhecida como *Great Firewall*.

4.4. Legislações Relacionadas à Internet na China

A partir de 2012, a internet passou a ser regulamentada por corporações privadas, conectadas ao governo via o *Internet Society of China* (ISC) que emitiu diretrizes em áreas como gerenciamento de blogs e mecanismos de pesquisa, comércio justo e direitos autorais. Com o crescimento da internet, a subdivisão das áreas de legislação se tornou obsoleta, já que as empresas não penalizavam os usuários. Neste cenário, foi promulgada a lei de responsabilidade civil para proteção dos direitos pessoais.

Em outubro de 2014 foi aprovada uma resolução sobre violação online dos direitos da personalidade, que prevê que a obrigatoriedade das empresas que operam virtualmente fornecerem aos tribunais nomes, endereços e métodos de contato dos usuários, quando as informações publicadas forem consideradas difamatórias. Em novembro de 2014, foi firmada o comprometimento dos desenvolvedores e lojas de aplicativos a ampliar a implementação de sistemas de autenticação de identidade.

O registro de identidade se estendia para a compra de telefones, permitindo a identificação de atividades online por meio das peças de hardware. Em fevereiro de 2015, o CAC exigiu um sistema de registro de nome real para todos os serviços de informação online baseados em contas. Também era exigido a introdução de avaliação por pontuação de comportamento individual online, que implicavam em listas de restrição para aqueles que apresentassem conduta considerada prejudicial.

Em vigor desde 2017, a Lei Nacional de Cibersegurança, conceitua a proteção de dados pessoais online como um direito civil fundamental, definindo parâmetros para a proteção destas informações. A lei aborda a estratégia e promoção da segurança cibernética, segurança de operações e informações de rede, monitoramento, alerta antecipado e respostas de emergência, responsabilidades legais e disposições complementares. Apesar de sua abrangência, a CSL não esclarece o papel do governo na proteção dos cidadãos (Yang & Xu, 2018).

4.5. A Influência Governamental e o Impacto na Internet no País

Considerando o "grande firewall da China", com administração e controle pela *CAC*, cujo atua no bloqueio de palavras-chave nas pesquisas e IP's da web na rede chinesa, é localizado o interesse dos assuntos bloqueados para pesquisa. Zittrain e Edelman (2003) apresentam em seus testes bloqueios como: "Tibet", "Taiwan" e "*Revolution"*, visto que os conflitos políticos pelos territórios citados vêm desde aquela época.

O sistema de pontuação de cidadãos na china, o *China's Social Credit System(s)*, o qual inicialmente havia sido criado para crédito bancários, garante acesso a conduta online e localização e contato com usuários acusados de difamação online, conforme a resolução sobre violação online de direitos da personalidade aprovada no ano de 2014.

Baseado na tríade CIA em seus tópicos de privacidade e confidencialidade, a centralização de tratamento de dados pelo governo chinês e monitoramento de conteúdos passiveis de acesso, a CSL afirma seu papel na promoção de cibersegurança, segurança de operações e informações de rede monitoramento, alerta antecipado e respostas de emergência, responsabilidades legais e disposições complementares. Entretanto, ela não esclarece o papel do governo neste processo e proteção de dados dos cidadãos.

4.6. Discussão

Há indícios de que a China aparenta estar interessada na criação de políticas de confidencialidade no país, como a criação da instituição CAC, da CSL – a lei chinesa para controle do tratamento de dados na internet - e a criação de direitos a privacidade, autores afirmam que a lei aparenta criar barreiras ao tratamento de dados apenas no setor privado (Yang & Xu, 2018).

Sites considerados “promotores da ocidentalização”, como o *Twitter* e o *Facebook*, são banidos ou modificados sem que haja, por parte do governo, uma justificativa objetiva, interferindo no conceito de disponibilidade (GREATFIRE, 2011). Neste contexto, pode-se identificar que as declarações do governo que afirmam obstruir o acesso apenas conteúdos danosos ao ambiente são contraditórios (Miao et al., 2018).

Ademais, existem termos bloqueados ou parcialmente ocultados, como o #MeToo, Massacre da Praça da Paz Celestial, Guerra e Revolução (Chung & Fu, 2022; Xiong & Ristivojević, 2021), que são inibidos das pesquisas de busca pelo governo, não condizente com as diretrizes de integridade e disponibilidade da informação pontuadas, mostrando-se como tópicos de que há interesse na mitigação da disseminação unicamente por parte dos órgãos de controle do governo.

A criação de direitos a privacidade, leis e departamentos de regulamentação da esfera virtual cria uma atmosfera de incerteza aos cidadãos sobre quais tópicos podem ser veiculados e acessados sem que haja interferência e sanções governamentais.

5. Conclusões

A influência governamental chinesa na indústria do país é clara, principalmente devido ao funcionamento do modelo econômico da China. Dentro deste controle, a segurança da informação é um tópico crescente de discussão entre a população chinesa e em congressos do governo em relação à internet. Um dos principais motivos são os questionamentos sobre privacidade e o aumento do número de ataques cibernéticos.

Conforme os dados acumulados no decorrer desta pesquisa, a China possui legislações internas fortes para que o setor privado garanta a confidencialidade, integridade e disponibilidade das informações pessoais acumuladas durante a prestação de seus serviços, porém muitos destes conceitos são ignorados pelo setor público e não há legislações específicas para o tratamento de dados pelo governo.

O presente estudo evidenciou como o tratamento de dados dos chineses garante os conceitos da tríade CIA. Algumas limitações foram encontrar estudos que analisassem o uso da CIA nas entregas de informações no país, e encontrar informações a partir de websites do próprio governo. Pesquisas posteriores podem analisar o tratamento de dados dentro das mídias sociais da China ou a adaptação de empresas estrangeiras na internet chinesa.

A contribuição apresentada para a teoria é a apresentação dos diferentes ambientes e as limitações importas a outros países quando em troca de dados com a China. A contribuição para a prática é de apresentar os principais desafios para os gestores que desejam empreender campanhas ou novos negócios em território Chinês e utilizarão da internet em seus projetos.

Referencial Bibliográfico

Cao, C., Suttmeier, R., & Simon, D. (2006). China's 15 Year Science and Technology Plan. *Physics Today*, *59*(12), 38–43.

CAS. (1996). *Obligations and Rights—ACADEMIC DIVISIONS OF THE CHINESE ACADEMY OF SCIENCES*. http://english.casad.cas.cn/Me/OR/200905/t20090515_3152.html

CCNIC. (2021). *The 48th Statistical Report on China's Internet Development* (Nº 48). China Internet Network Information Center. https://www.cnnic.com.cn/IDR/ReportDownloads/202111/P020211119394556095096.pdf

Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, *3*(3), 306–326. https://doi.org/10.1080/23738871.2018.1556720

Chung, R. W., & Fu, K. (2022). Tweets and Memories: Chinese Censors Come after Me. Forbidden Voices of the 1989 Tiananmen Square Massacre on Sina Weibo, 2012-2018. *Journal of Contemporary China*, *31*(134), 319–334.

Creemers, R. (2016). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, 85–100.

Diana, A., Tojeiro, C., Cardoso, T. M., Lucas, T. J., & Moraes, E. A. (2016). COMPUTAÇÃO EM NUVEM - DISPONIBILIDADE: PESQUISA APLICADA NA FACULDADE DE TECNOLOGIA DE OURINHOS. *RETEC - Ourinhos*, *9*(2), 75–79.

Fernandes, N. O. C. (2013). *Segurança da Informação*. e-TEC. https://www.fatecourinhos.edu.br/retec/index.php/retec/article/view/214

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital Identity Guidelines* (p. 1–104). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

GREATFIRE. (2011). *Censorship of Domains in China*. https://en.greatfire.org/search/domains

Guillermaz, Jacques. (1968). *Histoire du parti communiste chinois / Jacques Guillermaz*. Payot Paris. https://catalogue.nla.gov.au/Record/605270

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002.* (3º ed). Brasport.

ISO. (2013). International Standard Organization—ISO/IEC 27001. Em *ISO*. https://www.iso.org/standard/54534.html

Jiang, Min., & Fu, K.-W. (2018). Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit? *Policy & Internet*, *10*(4), 372–392. https://doi.org/10.1002/poi3.187

Majerowicz, E. (2020). A china e a economia política internacional das tecnologias da informação e comunicação. *GEOSUL*, *35*(77), 1–21.

Miao, W., Zhu, H., & Chen, Z. (2018). Who's in charge of regulating the Internet in China: The history and evolution of China's Internet regulatory agencies. *China Media Research*, *14*(3), 1+. Gale Academic OneFile.

Nonnenberg, M. J. B. (2010). China: Estabilidade e crescimento econômico. *Brazilian Journal of Political Economy*, 201–218.

Pomar, W. (2003). *A Revolução Chinesa*. Editora UNESP.

Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward Proper Authentication Methods in Electronic Medical Record Access Compliant to HIPAA and C.I.A. Triangle. *Journal of Medical Systems*, *40*(4), 100. https://doi.org/10.1007/s10916-016-0465-x

Xiong, J., & Ristivojević, D. (2021). #MeToo in China: How Do the Voiceless Rise Up in an Authoritarian State? *Politics & Gender*, *17*(3), 490–499.

Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *Asia & the Pacific Policy Studies*, *5*(3), 533–543. https://doi.org/10.1002/app5.246

Zittrain, J., & Edelman, B. (2003). Internet Filtering in China. *Berkman Center for Internet & Society*, 1–21.