XXVIII ENCONTRO NACIONAL DO CONPEDI GOIÂNIA – GO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

CARLOS VINÍCIUS ALVES RIBEIRO

D597

Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/ UFG / PPGDP

Coordenadores: Danielle Jacon Ayres Pinto

Aires Jose Rover

Carlos Vinícius Alves Ribeiro – Florianópolis: CONPEDI, 2019.

Inclui bibliografia

ISBN: 978-85-5505-803-5

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constitucionalismo Crítico, Políticas Públicas e Desenvolvimento Inclusivo

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVIII Encontro Nacional do CONPEDI (28 : 2019 : Goiânia, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
Univeridade Ferderal de Goiás e Programa
ePós-Graduação em Direito Florianópolis

Santa Catarina – Brasil
www.conpedi.org.br

UFG UNIVERSIDADE FEDERAL DE GOIÁS

PPGDP Programa de Pós-Graduação em Direito e Políticas Públicas

de Pós Graduação em Direito e Políticas Públicas
Goiânia - Goiás
https://www.ufg.br/

XXVIII ENCONTRO NACIONAL DO CONPEDI GOIÂNIA – GO

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

O XXVIII Encontro do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI) mostrou que os temas relacionados as novas tecnologias estão cada vez mais inseridos na realidade jurídica, social, política e econômica brasileira e do mundo. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e deixaram em evidência uma interconectividade de temas e áreas do conhecimento que demonstraram que a buscar por soluções nessa esfera só pode ser pensada de forma multidisciplinar e alicerçada na criatividade e inovação.

Todavia, apesar da diversidade dos temas, foi possível agregá-los em blocos de forma a aprimorar o debate e criar uma linha condutora para o grupo de trabalho.

Na primeira parte dos trabalhos os temas centraram-se no debate sobre acesso à informação e proteção de dados. Assunto altamente em voga hodiernamente, os trabalhos procuraram entender como está sendo pensada a privacidade, a segurança, a liberdade e a utilização dos dados de pessoas e empresas no espaço virtual. Quais legislações que versam sobre isso e como podemos entender seus alcances e lacunas foi o mote central dos estudos.

Na parte seguinte o tema versou sobre o Estados e a interação com as novas tecnologias. Na busca por desenvolver cada vez mais a digitalização das instituições, tanto públicas como privadas, os artigos desse bloco problematizaram as novas dinâmicas e atores do espaço digital e qual o papel do Estado na garantia da regulação e proteção desses novos entes e da própria sociedade.

O terceiro bloco trouxe um tema mais diretamente ligado ao mundo jurídico com o debate sobre a governança digital e a justech, ou seja, a justiça tecnológica tanto do ponto de vista burocrático, como da possibilidade da justiça feita por ferramentas digitais. Nesse bloco, os artigos buscaram pensar como entender a governança e os processos institucionais quando ferramentas digitais podem substituir o trabalho humano na esfera pública, em especial no poder judiciário.

Por fim o último bloco propôs um debate multidisciplinar centrado na biotecnologia, trazendo para o centro do debate questões relacionadas com energia, meio ambiente e o papel das tecnologias nessa seara. Os trabalhos procuraram discutir as novas ferramentas e

regulações na área da biotecnologia e como esses meios precisam ser cada vez mais utilizados para aprimorar a proteção e aumentar a inovação.

Com esses estudos de excelência os coordenadores desse excelente grupo de trabalho convidam a todos para ler na integra os artigos e aumentar o debate e a pesquisa nessa temática central da realidade jurídica, política, econômica, cultural e social do mundo contemporâneo.

Prof. Dr. Aires José Rover - UFSC

Prof. Dr. Carlos Vinícius Alves Ribeiro – PUC-GO

Prof. Dr. Danielle Jacon Ayres Pinto – IMM/ECEME e UFSC

Nota Técnica: Os artigos que não constam nestes Anais foram selecionados para publicação na Plataforma Index Law Journals, conforme previsto no artigo 8.1 do edital do evento. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

SEGURANÇA E DEFESA CIBERNÉTICA: UMA PERSPECTIVA DAS INICIATIVAS LEGISLATIVAS NA AMÉRICA DO SUL

SECURITY AND CYBER DEFENSE: A PERSPECTIVE OF LEGISLATIVE INITIATIVES IN SOUTH AMERICA

Danielle Jacon Ayres Pinto [1]
Riva Sobrado De Freitas [2]

Resumo

Desde do início do século XXI o Estado está sendo colocado frente a novas ameaças tanto para sua defesa como para a garantia de segurança de seus cidadãos. Nesse espectro uma das áreas mais sensíveis e produtoras de novos recursos de poder e violência no sistema, são as novas tecnologias, entre elas a internet. Frente a esse cenário, esse artigo se propõe a identificar quais as iniciativas legislativas na América do Sul e se de fato, elas estão sendo efetivadas numa rede de cooperação interestatal. A metodologia será exploratória-descritiva, usando análise qualitativa para entender as repercussões cooperativas desses elementos legais.

Palavras-chave: Ciberespaço, Segurança, Defesa, Legislação, América do sul

Abstract/Resumen/Résumé

Since the beginning of the twenty-first century, the State has been confronted with new threats both for its defense and for the security of its citizens. In this spectrum one of the most sensitive areas and producers of new resources of power and violence in the system are the new technologies, among them the Internet. In view of this scenario, this article proposes to identify the legislative initiatives in South America and if indeed, they are being implemented in an interstate cooperation network. The methodology will be exploratory-descriptive, using qualitative analysis to understand the cooperative repercussions of these legal elements.

Keywords/Palabras-claves/Mots-clés: Cyberspace, Security, Defense, Legislation, South america

[1] Professora da Universidade Federal de Santa Catarina - UFSC, Pós-doutoranda na Escola de Comando e Estado-Maior do Exército - ECEME, Coordenadora do grupo de pesquisa em Política Internacional GEPPIC (www.geppic.ufsc.br)

[2] Professora do PPGD em Direitos Fundamentais da UNOESC, Professora Aposentada da UNESP-Franca, Pós-Doutora em Direito Constitucional pela Universidade de Coimbra.

Introdução[1]

A realidade das relações entre os atores do espaço internacional, desde seus primórdios, é formada por um constante cenário de conflitualidade e busca por poder. Tal cenário vai, todavia, ter duas peculiaridades: a evolução dos recursos de poder utilizados pelos beligerantes, como também, a modificação das ameaças ao longo do tempo e de suas consequências diretas aos agentes.

Nesse sentido, o século XXI e as ações que o moldaram: fim da guerra-fria, globalização, surgimento da internet, ascensão de novos Estados influente, ascensão de grupos extremistas, táticas de promoção do terror no centro do mundo hegemônico, etc; vão mostrar ao mundo a necessidade de repensar os espaços de poder, seus recursos e as maneira de utilizá-los.

É frente a esse quadro que o ciberespaço surgirá como uma nova ferramenta que alimentará o poder dos atores, ao mesmo tempo em que, mudará a maneira como se relacionam e enfrentam seus dilemas internacionais.

A maneira como tais atores irão lidar com essa ameaças cibernéticas podem estar diretamente ligadas a uma dicotomia conhecida do sistema internacional: o reforço dos armamentos tradicionais como forma de garantir segurança ou, por outro lado, a tentativa de construir processos de cooperação onde o objetivo principal seja o fortalecimento da segurança coletiva.

Assim, esse artigo tem por objetivo repensar as bases do poder tradicional e como o ciberespaço influencia na sua conceituação contemporânea, demonstrar as principais ameaças que o meio digital promove ao sistema internacional e por fim, analisar as respostas legislativas que os atores estatais latino-americanos estão dando a essa realidade em forma de entendê-la como uma ameaça securitária que demande ações tradicionais ou não em sua contenção.

A abordagem metodológica desse trabalho se propõe a ser exploratória-descritiva, utilizando de pesquisa em fontes primárias e secundárias para fazer um levantamento das iniciativas mais importantes do ponto de vista legislativo nos países da América do Sul. Após

[1] Esse artigo faz parte dos resultados de pesquisa produzidos pelo Projeto "Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional" que é apoiado com recursos do Ministério da Defesa e CAPES através do edital Pró-Defesa de 2019.

esse levantamento a proposta é fazer uma análise qualitativa para compreender os caminhos securitários desses documentos legais, desse modo, nessa parte do artigo se utilizará da técnica de pesquisa comparativa, observando os documentos levantados e procurando semelhanças e distinções entre eles.

Importante ressaltar que o objetivo desse artigo é o levantamento dessas inciativas sulamericanas e a análise sobre quais os caminhos que estão sendo direcionadas, ou seja, se privilegiam mais a concepção de segurança cibernética ou de defesa cibernética. Essa conclusão observativa é de suma importância para entender se a perspectiva de relacionamento interestatal nessa esfera está sendo calcada em combate a ameaças e manutenção da sobrevivência do Estado de forma unilateral ou se os meios cooperativos estão sendo privilegiados dando ênfase a processos de formação de redes e de criação de arcabouços legislativos mais amplos e de alcance internacional.

1. Poder e o século XXI

Falar de poder é sempre algo complexo e que pode levar o(a) autor(a) a incorrer em erros constantes, isso se deve principalmente pela dimensão abstrata que tal conceito tem. Numa grande parte das vezes poder é confundido com recursos de poder, de forma que um ator ao possuir uma quantidade considerável de um determinado recurso de poder é automaticamente reconhecido como expoente dentro de um determinado sistema. Isso é de certo uma falácia (NYE, 2011; BALDWIN, 2016; STOPPINO, 2003). Poder envolve uma série de questões adjacentes e que de fato, precisam de um ato relacional para que os atores envolvidos vejam o resultado de seu poder se materializando, ou seja, poder está muito além do que somente posse de recursos (AYRES PINTO, 2016).

Dessa forma podemos entender poder na política internacional através de dois conceitos, um mais tradicional e apoiado nas teorias clássicas do pensamento internacional, e outro mais contemporâneo, arraigado na dinâmica tradicional do mundo pós-guerra fria.

Numa dinâmica tradicional temos a ideia de poder identificada por Max Weber (2004, p. 188) onde o autor indica que “poder é a possibilidade de impor a terceiros a vontade própria”. Essa conceituação vai permear grande parte das ações dos atores no espaço internacional, impor aos demais a sua vontade não é somente uma demonstração de força, mas também uma garantia de sobrevivência sob ótica de uma percepção realistas da prática da política no espaço externo.

Impor a vontade a outrem estará ligado a uma necessidade de possuir recursos de poder que possam garantir o sucesso dessa coerção, nesse sentido, os recursos privilegiados de posse serão em sua grande maioria os bélicos – aqueles que podem ameaçar, e de fato injuriar o outro de modo que esse medo os faça submeter-se a vontade de outro agente.

Essa percepção de poder, é vista na política internacional durante quase todo o século XX, com mais ênfase ao período da guerra-fria e da sua ideia de corrida armamentista como forma de vencer a batalha ideológica ali firmada. O autor americano Joseph Nye Jr. (2004) ao escrever sobre poder, passou a denominar esse tipo de poder como *hard power*. Assim, num processo de percepção de paz ou guerra, poder numa dinâmica realista é apoiador de um processo constante de rearmamento em prol não só de segurança, mas principalmente, de uma manutenção de controle e de um *status quo* do agente.

Todavia, as ameaças enfrentadas por esse tipo de poder são de certo ameaças reais, que possuem uma materialização no mundo real, ou seja, fora do espaço virtual. É possível compreender quantitativa e qualitativamente suas consequências e de certo modo, agir em prol de eliminar seu perpetrador.

Um outro conceito de poder perceptível na realidade internacional é aquele que se pode denominar de contemporâneo, muito por que sua efetivação terá sucesso no mundo pós-guerra-fria. Essa percepção de poder não abandona a vertente de coerção da matriz tradicional, mas diante de um mundo cada vez mais globalizado e interdependente, os atores detentores de poder, na sua maioria Estados-nação, são obrigados e utilizar-se menos da imposição e mais de um processo de mudança comportamental (NYE, 2011) de forma que mais do que recursos bélicos serão necessários recursos alternativos para construir influência.

Se numa dinâmica tradicional poder tinha por intuito impor a outro uma vontade, nesse momento contemporâneo tal imposição tem custos que mais prejudicam o ator estatal do que o auxiliam na construção do poder, e assim, eles preferem angariar aliados e provocar uma mudança no comportamento destes, do que impor a tal uma transformação a força e a consequência ser contrária (e desastrosa) para o Estado disseminador de poder (AYRES PINTO, 2016).

Nesse sentido, mais do que quais recursos de poder se possui o importante é como alcançar um certo fim pretendido com os recursos que se possui, ou seja, a preocupação é com os resultados e como converter recurso em poder (NYE, 2011). Deste modo, estratégias de

construção de poder, são mais importantes que a posse de recursos de poder, visto que sem o primeiro quaisquer recursos poderiam se tornar subaproveitados. Nye (2004) convencionou chamar esse tipo de poder de *soft power*.

No cenário político global contemporâneo, mais globalizado e interdependente, as ameaças que devem ser enfrentadas são mais sutis e, muitas vezes, mais letais do que as tradicionalmente enfrentadas anteriormente. Nesse meio as ameaças ultrapassam o mundo real e adentram a esfera virtual, e sendo a mesma um universo abstrato e sem fronteiras os tradicionais recursos de poder não mais alcançam os efeitos que anteriormente obtinham, e a própria ameaça não mais é facilmente identificável.

Vejamos brevemente um quadro que pode explicar essa dinâmica de poder:

Quadro 1 – Poder como recurso e como resultado comportamental

O PODER DEFINIDO COMO RECURSO
Contexto → Habilidade
Poder = recursos → estratégia de conversão → resultados preferidos
O PODER DEFINIDO COMO RESULTADOS COMPORTAMENTAIS
Poder = afeta outros → com referência a algo → por meio de → para resultados preferidos
[âmbito] [escopo] [coerção, recompensa, atração]

Fonte: NYE, 2011, p. 31

Nesse cenário dual entre o poder tradicional e o contemporâneo Joseph Nye (2010, 2011) vai ainda identificar uma nova dinâmica do poder que terá duas dimensões: uma transição do poder e uma difusão do poder. Essas duas dimensões serão responsáveis por, em partes, fazer com que os recursos cibernéticos passem a ser efetivamente um elemento de poder e que os Estados passem a ter uma preocupação com eles, tanto do ponto de vista de um ataque, mas principalmente, do ponto de vista da sua incapacidade em tornar esse recurso parte da sua capacidade de ação e influência no sistema.

Assim, para entender melhor essa dinâmica se faz mister explicar o que são essas duas novas dimensões. A transição do poder estaria ligada a ideia que no pós-guerra fria e com a virada do milênio o mundo presenciou a ascensão de novas atores estatais com capacidade de influenciar o sistema e ameaçar a tradicional hegemonia dos atores centrais. Países como Brasil,

Índia, China, África do Sul, Singapura, Indonésia e em partes a Rússia, ascenderam com capacidade decisória no sistema internacional, passando assim a exercer poder nesse espaço. Todavia, seus recursos para isso não eram os tradicionais, mas sim, a capacidade de construir uma nova estratégia de promoção de poder e influência que privilegiaria outros recursos que não os tradicionais, fazendo assim com que novas dinâmicas fossem criadas no sistema. Nesse sentido o poder transita das bases tradicionais, para as novas potências em emergência no sistema (NYE, 2010, 2011).

A segunda dimensão identificada como difusão do poder é o fator que promove nos dias de hoje uma das maiores instabilidades e inseguranças no sistema internacional. Com o fim da guerra fria o mundo presenciou o surgimento de uma série de atores no sistema internacional que não tinham nenhuma ligação com o Estado. Atores como organizações não governamentais, empresas, grupos terroristas entre outros, passaram a ter muita influência nas decisões globais e na própria dinâmica do sistema. Todavia, sua capacidade de adquirir recursos de poder era mais limitada do que a dos Estado, pelo menos, era até a chegada da internet e do aumento exponencial de sua utilização ao redor do mundo (NYE, 2010, 2011). Com fácil e barato acesso a esse recurso, esses novos atores, que são difusos, passaram a poder exercer poder no sistema e a ameaçar o Estados e os indivíduos de forma nunca antes vista, um exemplo disso foi o malware Ransomware[2] que atacou computadores mundo afora em 2017.

Será frente a esses dois modelos de poder, que não são antagônicos, mas sim complementares e a essa nova dinâmica de transição e difusão, que a resposta as ameaças cibernéticas terão que ser dadas. Frente a essa realidade, Estados terão que repensar suas estratégias de defesa e buscar entender se o rearmamento de suas forças bélicas será um meio mais eficaz para combater tais crimes, ou se a construção de um espaço de paz e cooperação terá mais efetividade no combate a essa nova ameaça virtual do século XXI, e o caminho para isso será na criação de elementos legais que versem sobre o tema cibernética e na sua direção podendo ser ela mais em prol de elementos de defesa ou mais em prol de elementos da segurança, ou então num processo que seja capaz de interconectar ambas dimensões.

[2] Para saber mais sobre malware e o sobre Ransomware consultar: https://www.foccoerp.com.br/gestao-de-ti/ransomware-virus-que-sequestra-arquivos/

2. Defesa Cibernética e Segurança Cibernética: ameaças contemporâneas

O mundo pós-guerra-fria experimentou uma série de novas dinâmicas tanto econômicas, como políticas e principalmente sociais. O advento da internet é um marco da última década do século XX e suas consequências uma herança deixada para ser tratada pelos atores que influenciam a cena política no século XXI. Assim, nessa parte se faz importante determinar o que se entende por espaço cibernético, defesa cibernética e segurança cibernética e como tais conceitos estão relacionados a percepção de segurança dos agentes internacionais, em especial o Estado.

Apesar do termo ciberespaço parecer algo diretamente ligado a internet e suas dinâmicas, é preciso desconstruir essa percepção, pois ela pode incorrer em erro. Segundo Cepik, Canabarro e Borne (2014, p. 162) ciberespaço é definido por "um domínio operacional marcado pelo uso da eletroeletrônica e do espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações através de redes interconectadas e interdependentes", esse conceito pode ser complementado pelo argumento de Kuehl (2009, p. 29) que diz que o ciberespaço é "[...] espaço onde humanos e suas organizações usam a tecnologia para agir e criar efeitos [...]". Diante dessas conceituações, ciberespaço é algo para além da internet, ou melhor, é algo que existe antes da internet. Os telégrafos, telefones, televisão por satélite, GPS e outros meios de troca de informação existem desde da metade do século XX e utilizam-se desse espaço visualmente abstrato para efetivar sua finalidade (CANABARRO, BORNE, 2013). Assim, esse espaço virtual por excelência já existe, mas a indagação pertinente hodiernamente é quando tal passará a representar uma ameaça aos atores estatais e um espaço de projeção para seu poder?

Um possível marco para essa resposta é a disseminação da internet como forma de comunicação e interação entre os indivíduos de todo mundo em meados da década de 90 do século XX. Se antes o espaço virtual era entendido e permeado por poucos atores, a Internet com sua função de interconexão entre computadores de todo mundo, abriu espaço para o surgimento de novos tipos de relações no sistema internacional, e com isso, também o surgimento de novos tipos de ameaças que não mais as tradicionais promovidos pelos atores estatais.

Se até a guerra fria as ameaças eram facilmente identificáveis e a segurança construída através dessa percepção, com o advento desse novo elemento a dinâmica relacional entre os agentes será afetada e tal dimensão será propositalmente securitizada na tentativa de criar um controle e antever ameaças, nesse momento veremos surgir o termo cibersegurança ou segurança cibernética. Segundo Oliveira, Gama Neto e Lopes cibersegurança é:

> Conjunto de medidas oriundas da segurança da informação – daí que os atributos de confidencialidade, integridade e disponibilidade são tidos como mais importantes, dentre aqueles imprescindíveis para salvaguarda da informação – adotados para o combate e a prevenção dos denominados crimes cibernéticos. No âmbito do poder público, tal conjunto é tomado no nível político; na iniciativa privada, pode ser implementada por qualquer indivíduo, grupo ou empresa. [...]

E completam

> [...] Todavia, seu uso em CiberRI parece se voltar mais para uma metáfora em que os elementos "segurança" (sensação de proteção de uma sociedade que necessita de mecanismo de Segurança e Defesa) e cibernética se unem sob um forte viés "securitizatório". (Oliveira; Gama Neto; Lopes, 2016, p. 208).

Segurança cibernética estaria assim muito mais ligada a ameaças direcionadas para a sociedade civil e menos para o Estado, sendo que a defesa cibernética estaria conectada com os recursos de poder do Estado e sua ameaça direta a soberania desse ator, sendo que as respostas, como o próprio dano causado, poderiam ter proporções mais drásticas quando se fala de defesa cibernética e suas ameaças.

Assim, o ciberespaço vai tornar-se algo relevante para dinâmica dos Estados e para a construção do seu poder, principalmente quando a Internet passa a promover novos meios de relação que geram ameaças para o *status quo* dos agentes estatais e colocam em cheque o próprio equilíbrio do sistema. Como vimos antes nesse artigo, o poder cibernético estará intimamente ligado a dois novos tipos de fenômenos no século XXI: a transição do poder e a difusão do poder. As ameaças estão mais fora do controle do Estado do nunca tiveram antes e, consequentemente, seus recursos de poder tradicionais passam a ter uma noção de anacronismo como ferramentas de enfrentamento a essa nova realidade de ameaças e controle do sistema internacional (NYE, 2010, 2011).

Nesse sentido, e de maneira breve, se faz importante nesse trabalho elencar os tipos de ameaça e conflitos que essa nova ferramenta digital irá produzir no sistema. Segundo Möckly (2012) são elas: hacktivismo, crime cibernético, espionagem cibernética, sabotagem cibernética, terrorismo cibernético e guerra cibernética.

Vejamos um quadro que tenta delimitar os possíveis delitos cibernéticos e classifica-los como segurança ou defesa cibernética

Quadro 2 - Ameaças cibernéticas e suas definições securitárias

Ameaças	Definição Securitária	
Hacktivismo	CIBERSEGURANÇA	Alvo principal é a área Privada/Sociedade Civil
Crime Cibernético		
Espionagem Cibernética	CIBERSEGURANÇA / CIBERDEFESA	Alvo principal é tanto a área Privada/Sociedade Civil como o setor Público
Sabotagem Cibernética		
Terrorismo Cibernético	CIBERDEFESA	Alvo principal é o setor público e suas infraestruturas críticas
Guerra Cibernética		

Fonte: AYRES PINTO, FREITAS, PAGLIARI, 2018, p. 49

Como é possível perceber, dificilmente o fortalecimento dos tradicionais recursos de poder será uma medida efetiva para enfrentar uma ameaça nova e que se coloca para além da tradicional compreensão de soberania e fronteira que os Estados possuem. Pode ser mais efetivo pensar em espaços regionais de paz mais cooperativos que ao interagirem construirão entre si uma resposta coletiva mais segura frente as ameaças digitais. Porém, com os últimos ataques cibernéticos ocorridos, é possível pensar que mais do que juntarem-se para se defender coletivamente, os Estados estão almejando criar da própria ferramenta cibernéticas armas contemporâneas de ataque a seus inimigos e com isso, mais do que elementos de promoção da paz, seriam tais recursos elementos de um tipo de rearmamento contemporâneo dos Estados. Todavia, essa é uma realidade ainda muito obscura e que precisa de mais luz para poder ser compreendida nas suas táticas e estratégias.

A seguir, o texto vai abordar algumas medidas legislativa que estão sendo tomadas nos países sulamericanos para enfrentar essa nova ameaça digital no sistema internacional.

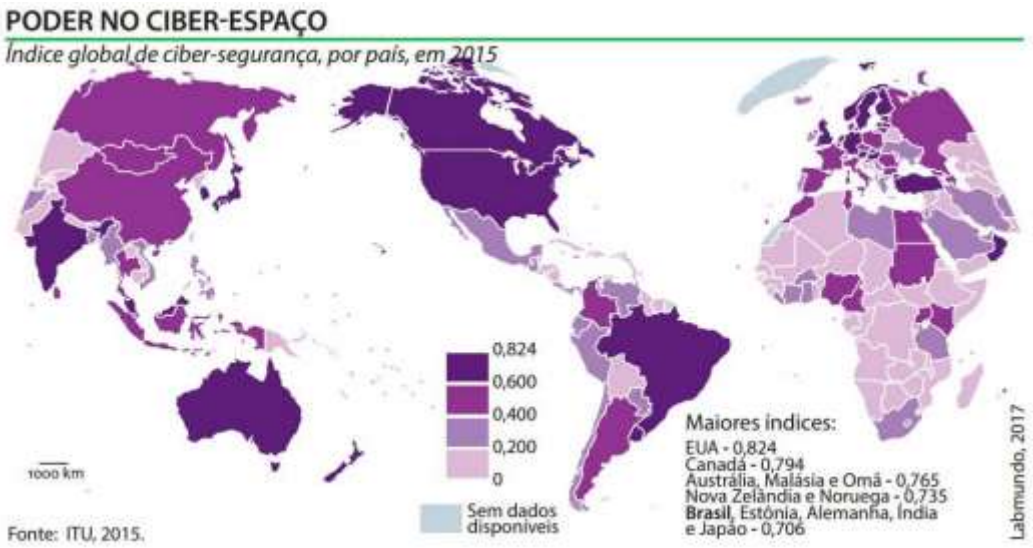
3. Iniciativas dos países sulamericanos para regular e combater as ameaças cibernéticas

As ameaças cibernéticas nos últimos anos, como se viu acima, tornou-se uma das questões centrais nas políticas de defesa e segurança dos Estados. Essa ameaça é capaz de atingir ao setor público e ao privado em dimensões muito semelhantes de estrago (respeitando obviamente a particularidade de cada esfera), o que forçou o ator estatal a criar políticas públicas de combate e prevenção para essa ameaça.

Nesse sentido, convém identificar de maneira inicial quais os principais documentos legais que tratam de defesa cibernéticas nos principais países da América do Sul e qual a perspectiva que possuem quando falam de recursos para enfrentar tal ameaça, ou seja, tais estratégias procuram meios tradicionais de defesa ou estão construindo alternativas de ação que podem privilegiar zonas de paz e cooperação.

Para definir quais países serão abordados de maneira inicial, se utilizará nesse ensaio o gráfico sobre poder no ciberespaço produzido pelo Atlas de Política Brasileira de Defesa (SOARES DE LIMA et. al., 2017).

Quadro 3 – Poder no Ciberespaço



Fonte: SOARES DE LIMA et. al., 2017, p. 48

De acordo com os dados do quadro acima, na América do Sul, por ordem de grandeza podemos identificar nove países em especial que possuem relevância na dinâmica do ciberpoder e da segurança cibernética, são eles: Brasil, Uruguai, Argentina, Colômbia, Paraguai, Chile, Venezuela, Peru e Equador.

Desta forma, iremos abarcar aqui, por escolha metodológica, os quatro mais relevantes e tentar entender quais são as suas políticas para a do ciberespaço. São eles: Brasil, Uruguai, Argentina e Colômbia.

3.1 Brasil

O Brasil é o mais extenso e populoso país da região, o que o faz, numa dinâmica de utilização de rede mundial de computadores ser um dos mais atuantes e isso o coloca com um dos mais visados a ataques e delitos cibernéticos (OEA; BID, 2016; TREND MICRO, 2013).

Suas respostas a essas ameaças são tanto de cunho público como privado. Todavia, na esfera pública a dinâmica de atuação nessa área ficou a cargo dos documentos de defesa e segurança nacionais e dos agentes que a eles estão ligados. Nesse sentido, um dos principais documentos a tratar de defesa cibernética no Brasil foi a Estratégia Nacional de Defesa em 2008, que colocou esse assunto sob os auspícios das forças armadas nacionais, em especial o Exército Brasileiro. Após esse início outros documentos foram produzidos e tratam do tema cibernético, são eles: o Livro Verde de Segurança Cibernética de 2010, o Livro Branco de Defesa de 2012 e a Política Nacional de Defesa de 2013 (SOARES DE LIMA et. al., 2017).

Como consequência da atuação do Exército brasileiro nessa área foi criado em 2010 o Centro de Defesa Cibernética (CDCiber) e que exerce um grande papel na proteção do Brasil nessa área e foi crucial para impedir ataques durantes os grandes eventos esportivos e políticos que aconteceram no Brasil entre 2012 e 2016.

Nos documentos do Brasil é possível ver uma ênfase significativa a ideia de identificação das vulnerabilidades do sistema e de adoção de medidas preventivas para combater tais fragilidades. Dilma Rousseff em discurso na ONU em 2013, vai dar o tom da ação do Brasil nesse sentido, deixando de certa forma explícito que o objetivo do país é evitar que esse espaço seja instrumentalizado como arma de guerra: “[...] evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio de espionagem, da sabotagem, dos ataques contra sistema e infraestruturas dos países. [...]” (ROUSSEFF, 2013, s/p).

Todavia, apesar de não ser identificada como uma ação de segurança ou defesa cibernética a legislação mais efetiva nessa área no Brasil é o Marco Civil da Internet, a lei N° 12.965/14 que tem por intuito criar um arcabouço legal de utilização e garantias tanto ao

cidadão como ao Estado na utilização da internet e a lei nº 12737/12 que tipifica criminalmente delitos informáticos.

Nessa forma, apesar do controle protetivo do ciberespaço no Brasil estar nas mãos de uma força militar, a ação em volta desse tema visa mais a criação de ferramentas digitais de proteção do que da utilização de forças bélicas como recurso de ação. Como afirmam Oliveira et.al. (2017, p. 68) "[...] O Brasil tem regulações e leis limitadas sobre o tema (cibernética) [...] apesar de a Constituição Federal e do Código Civil abordarem temas da privacidade, o debate sobre proteção de dados é recente".

3.2 Uruguai

O Uruguai apesar de ser o país menos populosos e extenso da região sulamericana é um expoente em utilização do ciberespaço, com uma alta taxa de penetração em sua sociedade das chamadas TIC (Tecnologias de Informação e Comunicação). Nesse sentido, junto com o Brasil ele se torna na região um dos pais poderosos agentes com poder no ciberespaço (OEA; BID, 2016).

Todavia, suas respostas de proteção a ataques do cibernéticos estão mais ligados a uma dinâmica de desenvolvimento e gestão eletrônica, do que necessariamente a uma ideia de defesa nacional. Nesse sentido, o Decreto Presidencial de 2009 de n. 452 convida todas as entidades governamentais a desenvolver políticas de segurança cibernéticas, dando ênfase a proteção de seus documentos e ao desenvolvimento de legislação de controle e de pessoal para agir nesse cenário.

Não há no Uruguai uma estratégia de defesa específica para o espaço cibernético, todavia, tal país é o maior expoente regional na produção de softwares de proteção a crimes digitais (OEA; BID, 2016). Porém o país possui um Livro Branco de Defesa onde tema da defesa cibernética e segurança cibernética são abordados numa clara identificação desse recurso como uma ameaça aos Estados, como também, o próprio documento assume o compromisso de pensar o tema de modo securitário em cooperação com os demais países da OEA. Para o Uruguai desenvolver capacidade tecnológica em conjunto com gestão pública diminui sensivelmente as vulnerabilidades do Estado frente a essas novas ameaças (OLIVEIRA et.al. 2017).

Assim, é possível perceber que no mesmo caminho que o Brasil, o Uruguai está criando mecanismo de cooperação e proteção dos seus dados, ao invés de investir em recursos bélicos para responder a ameaças.

3.3 Argentina

A Argentina é um dos países mais importantes do cone sul, porém, como destacado no quadro 3, seu ciberpoder fica abaixo do Brasil e Uruguai. Todavia, isso não a coloca como menos importante quando o assunto é proteção regional a ciberataques.

O país não é um dos principais alvos de ataques cibernéticos na região, todavia, é um dos primeiros Estados a pensar e institucionalizar ações para essa área no cone sul (GASTALDI; JUSTRIBÓ, 2016). Sua primeira iniciativa para segurança cibernética foi em 1994 com a criação do CSRIT Centro de Cibersegurança[2] e suas forças armadas fazem constantes exercício de resposta a ataques cibernéticos para desenvolver melhores métodos de ação e controle. Porém, a crítica maior dada a capacidade Argentina, principalmente de suas Forças Armadas é sua baixa capacidade de resiliência frente a um ataque (OEA; BID, 2016).

Nos últimos anos o governo argentino vem aprimorando medidas institucionais para fortalecer sua política de segurança cibernética, dando ênfase principalmente a definição de duas grandes áreas para pensar o ciberespaço: a do desenvolvimento tecnológico e a do processo de entender a dinâmica ciber na perspectiva da Defesa Nacional (GASTALDI; JUSTRIBÓ, 2016).

No pais efetivamente não ainda livros brancos ou estratégias nacionais de defesa que pensem sobre ameaças cibernéticas, todavia, há três instrumentos legais que colocam a Argentina como importante promotor de legislação nessa seara na América do Sul, são esses documentos: a lei nº 25.326/2000 que trata de privacidade e proteção de dados virtuais, da lei n.º 26.388 que cria punições as violações tipificadas na lei anteriormente citada e a resolução nº 580/2011 que foi elaborada pela *Jefatura de Gabinetes de Ministro*[3] e tenta versar sobre meios de proteção para ataques a infraestruturas críticas de informação, sendo então um documento mais ligado a defesa cibernética. (OLIVEIRA et.al. 2017).

Nesse sentido, igualmente aos países precedentes a Argentina nesse estudo, esse Estado busca muito mais um aprimoramento de suas redes de proteção do que necessariamente

[3] Para saber mais sobre esse órgão do governo Argentino consultar: https://www.argentina.gob.ar/jefatura

o aumento de seu potencial bélico para enfrentar essa ameaça, todavia, a questão relevante ainda quando se fala na Argentina é suas ações ainda estarem aquém das suas necessidades nessa área.

3.4 Colômbia

O país é um dos expoentes da região, é o segundo mais populoso depois do Brasil e nos últimos anos, com um processo de paz institucionalmente bem-sucedido, vem experimentando cada vez mais importância e relevância no cenário regional.

Todavia, suas ações para as ameaças do ciberespaço ainda são recentes, mas o seu fluxo de utilização de TIC demonstra sua importância e poder nessa área. O principal documento que trata sobre o ciberespaço e cibersegurança no país foi aprovado em 2016 é a sua Política Nacional de Segurança Digital – CONPES 3701. O documento tem por intuito reforçar as medidas para a criação cada vez maior de marcos institucionais de proteção a ameaças do ciberespaço (OEA; BID, 2016).

Porém, apesar da ideia de ameaça a segurança nacional por parte dos meios digitais ainda ser menor que as tradicionais ameaças – provindas de seu longínquo conflito civil) – quando o tema é a proteção privada, vemos que as ações são mais prolíferas, com o ColCert (um comitê de resposta a ameaças cibernéticas urgentes) funcionando em alto nível para proteção tanto privada como pública e leis que tratam de temas específicos dessa seara. Vejamos, a lei nº 529/1999 que fala sobre comércio eletrônico, a lei nº 1.150/2007 que fala sobre transparência e a lei nº 1.273/2009 que adequa o código penal frente a realidade cibernética.

O pais também possui alguns decretos, circulares e resoluções que versam sobre segurança cibernética, são eles: circular nº 52/2007 fala sobre qualidade de redes, resolução nº 2.258/2009 que trata do tema de regulação dos provedores, das redes e serviços de telecomunicações, o pais possui também o decreto n.º 2.758/2012 e a resolução n.º3.933/2013 que buscam tratar dos temas de defesa cibernética, mas são documentos mais organizacionais do que efetivamente promotores de marcos regulatórios efetivos. (OLIVEIRA et.al. 2017).

Nesse sentido, o país igualmente com os três anteriormente citados não objetiva enfrentar essa nova ameaça reforçando seus meios tradicionais de ação, mas sim, procurando novas formas de cooperação e definição de ameaças – como informa seu CONPES 3701 e

desenvolvendo novas ferramentas de proteção que não mais as tradicionais. Todavia, é fato a Colômbia possui uma iniciativa legislativa *a priori* mais quantitativa que seus congêneres regionais, todavia, não há como medir se isso resulta em melhor proteção, visto não ser esses dados produzidos de maneira efetiva pelo pais que durante os últimos 30 anos esteve voltado para o seu conflito interno e suas dinâmicas.

4. Considerações Finais

Esse artigo teve como fazer um levantamento sobre as iniciativas legislativas na área cibernética no espaço da América do Sul. Para tanto, foi preciso de fato debater as mudanças de poder na esfera internacional no século XXI e tentar compreender como os meios cibernéticos podem estar relacionados a esse cenário. O texto colocou como foco perceber se a respostas dos Estados a essas mudanças estavam ligadas a um reforço de seus armamentos tradicionais ou se estavam sendo construídas em modelos de cooperação como uma melhor forma de dar resposta a tal ameaça. Por fim, a ideia era iniciar um mapeamento das iniciativas legislativas dos países sulamericanos nessa área visando sua proteção e a criação de estratégias de enfrentamento do problema, tendo em vista a utilização dos seus recursos de poder nessas ações.

Por outro lado, a proposta desse artigo também foi fazer uma comparação entre os instrumentos legais dos países sulamericanos e tentar perceber se esses caminham mais para uma esfera de segurança cibernética ou defesa cibernética.

Na questão do poder foi possível perceber que as dinâmicas pós-guerra fria, tanto políticas, econômicas como sociais, trouxeram novas nuances para a realidade do sistema internacional e para seus atores. Num cenário com novas ferramentas de interação, produção de informação e comunicação o poder sofrer mudanças. As principais mudanças percebidas foram uma transição e um difusão do poder no século XXI, como identificou Nye.

Há mais Estados com poder e há mais atores exercendo poder no sistema.

Frente a essa realidade, também tentamos mapear quais as iniciativas legislativas dos países sulamericanos para se proteger frente as novas ameaças digitais. Escolhemos quatro países em específico – Brasil, Uruguai, Argentina e Colômbia – pela sua classificação numa ideia de ciberpoder determina por Maria Regina Soares de Lima e um grupo de pesquisadores em seu Atlas de Política de Política de Defesa Brasileira de 2017.

Nesse sentido o que inicialmente foi possível perceber é que os quatro países em questão estão atualmente cada vez mais comprometidos na promoção de instrumentos institucionais de segurança e defesa cibernética em seus territórios, e que esses envolvem uma série de atores do legislativo, do setor privado e principalmente do setor militar. Todavia, a proposta desses países não pareceu ser um rearmamento como forma de enfrentar tais ameaças, mas sim um reforço tanto nas suas capacidades digitais como humanas para melhorar suas dinâmicas tecnológicas nacionais e na criação de dispositivos cada vez mais institucionalizados que produzam marcos legais de ação estatal e privada na área de proteção a crimes cibernéticos e suas consequências.

Numa perspectiva comparativa, foi possível perceber que os países em questão estão me descompasso entre si frente as iniciativas legislativas. Apesar de todos já estarem produzindo documentos efetivos nessa seara, os caminhos não são uníssonos, mas sim, numa individual de compreensão e resposta frente as possíveis ameaças. Desse modo, mesmo que os conteúdos dessas iniciativas legislativas não visem entender os recursos cibernéticos como novas armas do Estado, também não visam criar uma rede cooperativa que entenda esse problema numa dinâmica regional que poderia, caso fosse feita, produzir uma dinâmica de proteção mais robusta e efetiva em todo cone sul.

Por fim, salientamos que esse estudo não se encerra em si mesmo, muito pelo contrário, ele é o início de uma jornada que pretende cada vez mais entender os recursos cibernéticos como os novos promotores de ameaças no sistema internacional, mas também, como um efetivo espaço para o aprimoramento das redes cooperativas entre os Estados visando diminuir os riscos securitários do novo milênio.

5. Referência Bibliográfica

AYRES PINTO, D.J.; FREITAS, R.S., PAGLIARI, G. C. 2018. *Fronteiras virtuais: um debate sobre segurança e soberania do estado*. In.: AYRES PINTO, D.J, FREIRE, M.R., CHAVES, D. S. **Fronteiras Contemporâneas Comparadas: desenvolvimento, segurança e cidadania**. Macapá: Editora da UNIFAP, 40-53.

AYRES PINTO, Danielle Jacon Ayres. *O smart power como um novo projeto de poder na esfera internacional: uma análise do Brasil e sua inserção internacional nos governos de Fernando Henrique Cardoso e Luiz Inácio Lula da Silva*. **Tese (Doutorado em Ciência**

Política) – Instituto de Filosofia e Ciências Humanos/IFCH da Universidade Estadual de Campinas – UNICAMP. Campinas, Brasil, 2016. Disponível em: http://repositorio.unicamp.br/jspui/handle/REPOSIP/305057

BALDWIN, D. A. **Power and International Relations: a conceptual approach**. New Jersey: Princeton University Press, 2016.

CANABARRO, D.R; BORNE, T. *Ciberespaço e Internet: Implicações Conceituais para os Estudos de Segurança*. **Boletim Mundorama**, n. 69, 2013, p. 1-5.

CEPIK, M.; CANABARRO, D.; BORNE, T. 2015. *A securitização do ciberespaço e o terrorismo: uma abordagem crítica*. In: MELLO e SOUZA, A.; NASSER; R. M.; MORAES; R.F. (org). **Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI**. São Paulo: IPEA, 161-186.

GASTALDI, S.; JUSTRIBÓ, C. *As estratégias de segurança e defesa cibernéticas na Argentina*. In: OLIVEIRA, M.A.G. (de); GAMA NETO, R.B.; LOPES, G. V. (org). **Relações Internacionais Cibernéticas (CibeRI): oportunidades e desafios para os estudos estratégicos e de segurança internacional**. Recife: Editora UFPE, 2016.

KUEHL, Dan. *From Cyberspace to Cyberpower: Defining the Problem*. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry**. Cyberpower and National Security**. Washington, Estados Unidos: National Defense University Press, 2009.

MÖCKLI, D. **Strategic trends 2012: key developments in global affairs**. Zurich: Center for Security Studies (CSS), 2012.

NYE (Jr.), J. S. **Soft Power: The means to success in World Politics**. New York: Publicaffairs, 2004.

NYE (Jr.), J. S. **Cyber Power**. Cambridge: Belfer Center for Science and international Affairs (Havard – Kennedy School), 2010.

NYE (Jr.), J. S. **The future of Power**. Nova Iorque: Public Affairs, 2011.

OEA; BID**. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?** Washington: OEA, 2016. Disponível em: https://publications.iadb.org/handle/11319/7449?locale-attribute=es&.

OLIVEIRA, M.A.G. (de); GAMA NETO, R.B.; LOPES, G. V. (org). **Relações Internacionais Cibernéticas (CibeRI): oportunidades e desafios para os estudos estratégicos e de segurança internacional**. Recife: Editora UFPE, 2016.

OLIVEIRA, M.A.G. de et.al. **Guia de Defesa Cibernética na América do Sul**. Recife: Editora da UFPE, 2017.

ROUSSEFF, D. **Discurso na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas**, 2013. Disponível em: www.planalto.gov.br.

SOARES DE LIMA, M. R. et al. **Atlas da Política Brasileira da Defesa**. Buenos Aires: CLACSO; Rio de Janeiro: Latitude Sul, 2017.

STOPPINO, M. Poder. In: Norberto Bobbio et al., **Dicionário de Política.** Brasília: UNB, 2003, p. 933-943.

TREND MICRO. **Brasil: Desafios de Segurança Cibernética Enfrenta por uma Economia em Rápido Crescimento**, 2013. Disponível em: http://www.trendmicro.com.br/cloud-content/br/pdfs/home/wp-brasil-final.pdf.

WEBER, M. **Economia e Sociedade – fundamentos da sociologia compreensiva**. Brasília: Editora UNB, 2004. V.2.