RDBCI: Revista Digital Biblioteconomia e Ciência da Informação
RDBCI : Digital Journal of Library and Information Science
DOI 10.20396/rdbci.v15i3.8647632

PARA UMA POLÍTICA DE INFORMAÇÃO NO CIBERESPAÇO: AVANÇOS, PERSPECTIVAS E DESAFIOS

FOR A CYBERSPACE INFORMATION POLICY:
ADVANCES, PERSPECTIVES AND CHALLENGES

PARA UNA POLÍTICA DE INFORMACIÓN EN EL CIBERESPACIO:
AVANCES, PERSPECTIVAS Y DESAFÍOS

[1]Jakeline Amparo Villota Enríquez, [2]Mardochée Ogécime, [1]Maribel Deicy Villota Enríquez, Heriberto González Valencia

[1]Universidad Santiago de Cali, [2]Universidade Federal da Bahia

Correspondência
[1]Jakeline Amparo Villota Enríquez
Universidad Santiago de Cali
Cali, Colômbia
Email: javillota@hotmail.com
ORCID: http://orcid.org/0000-0003-3086-8268

Submetido em: 23-11-2016
Aceito em: 02-06-2017
Publicado: 26-06-2017

JITA: LH. Computer and network security.

RESUMO: O presente artigo consiste em descrever e analisar as políticas da informação no ciberespaço, tanto global como regionalmente, em diversas direções: programas, resoluções e projetos do setor informacional. Igualmente, se apresenta um panorama das mesmas na região Latino-Americana e o Caribe. Mediante uma análise documental da literatura relacionada com o tema, o artigo se fundamenta numa revisão de literatura levantada a partir de materiais científicos. Em consequência, conceitua-se o ciberespaço e caracterizam-se seus elementos, dimensões, estratégias e variações, analisando as políticas da informação do ciberespaço, partindo do cenário global para relacioná-lo, finalmente, com o da região da America Latina e do Caribe, com a ideia de abordar melhor a problemática. As políticas de Informação do Ciberespaço experimentam diferentes progressos em matéria da cibersegurança y temáticas relacionadas com as mesmas; resultantes das politicas da informação estabelecidas por cada Estado o Região.

PALAVRAS-CHAVE: Políticas de informação. Ciberespaço. Cibersegurança. Cibersociedade.

ABSTRACT: This article is to describe and analyze the policies of information in cyberspace, both global and regionally, in different directions: programs, resolutions, and projects from the information sector. Likewise, an overview of the same is presented in the Latin American and Caribbean region. Through documentary analysis of the literature related to the topic, the article is based on a review of literature raised from scientific materials such as: books, thesis papers, dissertations, texts on internet sites and articles, resolutions, projects and decrees dealing with the same topic. As a result, cyberspace is conceptualized and its elements, dimensions, strategies and variations are characterized, by analyzing the information from cyberspace policy, based on the global stage to relate it, finally, to the region of Latin America and the Caribbean, with the idea of better addressing the problems. The cyberspace information policy experience a minor and slow process in the field of cyber war; resulting from the obstacle of international cooperation defined by the disparate ambitions of the State or region.

KEYWORDS: Information policy. Cyberspace. Cyber security. Cyber society.

RESUMEN: Este artículo consiste en describir y analizar las políticas de la información en el ciberespacio, tanto global como regionalmente, en diversas direcciones: programas, resoluciones y proyectos del sector informacional. Igualmente, se presenta un panorama de las mismas en las regiones Latino-Americanas y el Caribe. Mediante un análisis documental de la literatura relacionada con el tema, este artículo se fundamenta en una revisión de literatura levantada a partir de materiales científicos. En consecuencia, se conceptualiza el ciberespacio y se caracteriza sus elementos, dimensiones, estrategias y variaciones, analizando las políticas de la información del ciberespacio, partiendo del escenario global para relacionarlo, finalmente con el de la región de América Latina y del Caribe, con la idea de abordar mejor la problemática. Las políticas de la Información del Ciberespacio experimentan diferentes progresos en materia de la ciberseguridad y temáticas relacionadas con las mismas; resultantes de las políticas de la información establecidas por cada Estado o Región.

PALABRAS CLAVES: Políticas de información. Ciberespacio. Ciberseguridad. Cibersociedad.

1. INTRODUÇÃO

A transversalidade da informação e o uso das TIC em todos os setores que constituem o coração da vida nacional, como: transportes, energia, universidades, bibliotecas, usinas nucleares, cultura, economia, o setor informacional propriamente dito, etc., levaram à criação de um novo lugar desterritorializado, ou seja, o "ciberespaço". Como qualquer lugar, à pertença da competência do Estado, onde registram, circulam, armazenam, e operam as diversas informações do Estado - Nação, ele requer uma atenção especial de todas as forças vivas de uma Nação. No entanto, por sua abrangência, ele se transformou em um desafio de controle por parte dos estados, governos, atores decisórios no campo da informação, legisladores, etc. postos que os seus elementos constituem tanto os parâmetros estratégicos a serem tido em conta pelos Estados como as ações a serem levantado através de uma cooperação regional, nacional e/ou internacional.

Esse espaço, materializado pela internet como ferramenta de Tecnologia da Informação e Comunicação, converte-se em um suporte indispensável da "globalização", da economia capitalista e informacional; também, é entendido como um dos vetores de disseminação da democracia, dos valores e da liberdade de expressão. No entanto, constitui-se em uma ferramenta hegemônica e de poder, onde a questão da privacidade e a soberania dos Estados são constantemente discutidas. O ciberespaço institui, por tanto, um espaço de conflito posto que seja onde se desenvolvem a criminalidade, o terrorismo, a concorrência entre as empresas, indivíduos, ideias, poderes do Estado e militares Vera (2004).

Assim, hoje, pode-se dizer que a interdependência que caracteriza o sistema internacional nutre as relações criadas pelo ciberespaço. Apesar das vantagens envolvidas, esta dependência em tecnologia da informação deixam os Estados e a sociedade muito mais vulneráveis a vários tipos de ataques: intrusões e ataques informáticos, ciberterrorismo, espionagem de outros Estados, etc.

Neste sentido, KEMPF (2012, p. 7) argumenta que: "o ciberespaço apresenta características ***ambíguas*** e marcam uma ruptura com as fronteiras tradicionais no sentido de uma ***universalidade dos riscos***". Neste sentido, não existe uma distribuição homogênea sobre as caraterísticas do ciberespaço; pelo contrário, pode-se dizer que, para a maioria dos atores o ciberespaço apresenta diferenças significativas de estrutura, que impactam as condições de segurança. Os interesses e disparidades entre os diversos atores, países, e, até as mesmas regiões são fatores relevantes a serem levados em conta.

É importante ressaltar, para a compreensão do presente artigo que o conceito das "Políticas de Informação" se refere a "uma serie de princípios e estratégias que orientam um curso de ação para alcançar um objetivo" (MONTVILOFF, 1990, p. 11). Assim, as políticas da informação podem ser consideradas como um marco orientador para a ação de um

programa, plano ou atividade. Note-se que, a política, se assume como a decisão do governo, a qual pode ser legislável ou não.

O presente artigo consiste em descrever e analisar as políticas de informação do ciberespaço, tanto global como regionalmente, em diversas direções: programas, resoluções, projetos do setor informacional. Igualmente, se apresenta um panorama das mesmas na nossa região Latino-Americana e o Caribe. Por isso, se busca conceituar o termo "Ciberespaço" e caracterizar seus elementos, dimensões, suas estratégias e variações, como espaço além do virtual, pondo ênfase sobre as diversas abordagens políticas tanto globais como regionais e, analisando os seus impactos na sociedade Latino-Americana e o Caribe.

Pois, é necessário saber as iniciativas tomadas pelos governos, organizações não governamentais, instituições tanto ao nível global como regional para promover a segurança no contexto da atual Sociedade da Informação. Da mesma forma, entender as dimensões destas Políticas de Informação permite criar competências na resolução dos problemas do setor informacional no seu contexto da revolução digital e, estar informado sobre as iniciativas destinadas a regular o ciberespaço em um país ou uma região, a qual permitirá que os tomadores de decisões, usuários e profissionais da informação estejam conscientes do que acontece no seu ambiente com a finalidade de serem verdadeiros agentes de mudanças.

A metodologia aplicada neste estudo consistiu em uma análise documental da literatura relacionada com o tema, tanto na escala mundial como regional, para que a partir desta perspectiva, possa-se entender melhor o âmbito de ditas políticas de informação. Esta pesquisa se fundamentou numa revisão de literatura e em uma descrição das políticas globais e regionais existentes, suas procedências, especialmente as suas aplicações, para assim, conhecer seus impactos sobre a cibersociedade.

2. O QUE É O CIBERESPAÇO?

Basicamente, o termo "Ciber" evoluiu a partir da obra de Norbert Wiener (1948), que conceituou a "cibernética" como o "controle e comunicação do animal e da máquina". A ideia subjacente é que os humanos podem interagir com as máquinas e que o sistema resultante fornece um ambiente alternativo de interação, que por sua vez, proporciona a base do conceito do ciberespaço. Daí, no início dos anos 1980, o autor que aborda a ficção científica, William Gibson (1984), usou o termo ciberespaço em um de seus livros, "Neuromancer". Assim, esta palavra se espalhou nos círculos profissionais e acadêmicos, pelo que, durante anos, tem havido muitas e diferentes definições do ciberespaço dependendo das preocupações e interesses dos atores ou autores.

Por exemplo, o autor Gómez (2012) citou a definição do Departamento de Defesa dos Estados Unidos da América, que considera o ciberespaço como:

> Um domínio global dentro do ambiente da informação que consiste em uma rede interdependente de infraestruturas de Tecnologias de Informação (TI), incluindo as redes de Internet, telecomunicações, sistemas de computador e processadores embutidos e controladores. (GÓMEZ, 2012, p. 170).

De acordo com Ottis e Lorents (2011, p.4), a Comissão Europeia definiu vagamente o ciberespaço como "Um espaço virtual onde circulam os dados eletrônicos dos computadores do mundo".

Entretanto, na sua lógica mercantilista em apoio à iniciativa privada, a União Internacional de Telecomunicações (UIT), concebe o ciberespaço como um lugar criado através da interligação dos sistemas informáticos mediados pela Internet. De fato, o ciberespaço inclui:

> Usuários, redes, dispositivos, software, processos, informação armazenada ou corrente, aplicações, serviços e sistemas que estão direta ou indiretamente ligados a redes cuja segurança depende de um conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de risco, ações, formação, melhores práticas, seguros e tecnologias que podem utilizar-se para proteger os ativos de uma organização e usuários no ciberespaço [...]. Por isso, deve-se garantir que se alcance e manter as propriedades de segurança dos ativos da organização e os usuários contra os riscos de segurança correspondentes no ciberespaço. As propriedades de segurança incluem um ou mais dos seguintes: disponibilidade; Integridade, que podem incluir autenticidade e não repúdio; e confidencialidade. (UIT, 2008, p.6-7).

Segundo Douzet (2014), os russos, como os chineses, usam pouco o termo "ciberespaço" ou da ideia de um espaço além das fronteiras, e preferem falar da Internet ou da segurança da informação, levando as discussões no campo da competência dos Estados. Neste sentido, se refere à Internet, mais precisamente, como a interconexão global de equipamentos de tratamento automatizado de dados digitais. Os sistemas de informação e comunicação não se limitam à internet, mas é a Internet que tem dado origem ao que hoje é concebido como "ciberespaço".

Desta maneira, dentro deste artigo assumira-se o "ciberespaço" como aquilo que se refere tanto à Internet como ao espaço que ela gera: um espaço imaterial no qual se operam trocas desterritorializadas, entre os cidadãos de todas as nações, em uma velocidade instantânea que abole qualquer noção de distância. Assim, tecnicamente, reconhecemos que a Internet é a rede mundial de computadores que conecta inúmeras redes autônomas, usando a mesma linguagem de sistema. A qualificação do espaço que ela gera, é sujeita às representações contraditórias, ativismo, política, geopolítica, etc.

Partindo desta perspectiva, vários autores acham que a internet e o ciberespaço são agora realidades incontornáveis no mundo contemporâneo e na geopolítica. Os recentes acontecimentos têm enfatizado as suas importâncias na segurança das informações nacionais. Neste sentido, Robine e Salatian (2014, p. 123) afirmam que:

> A Internet é uma rede construída sobre o real, constituída de fibras ópticas, links de satélite e máquinas que estão localizados no espaço terrestre; o ciberespaço inclui as aplicações que exploram a Internet e parecem escapar do espaço de terra, de modo a formar um novo.

1.1 Ciberespaço: uma arquitetura em camada

Para entender melhor o Ciberespaço, evoca-se, às vezes, a sua estrutura em camadas. Isso permite decompor o ciberespaço como um milefólio cujas diferentes camadas podem interagir umas com as outras (BRUNO, 2000). Segundo os autores, pode-se dividir em duas, quatro, cinco ou sete camadas. E em todas as camadas desta estrutura há rivalidades de poder entre atores sobre questões muitas vezes altamente técnicas, cujos limites são ainda muito geopolíticos. Para simplificar, se apresentam, a seguir, as quatro camadas, baseando-se na perspectiva de Bruno (2000):

a) A primeira camada é **física**, a qual está composta por cabos submarinos e terrestres, uma verdadeira coluna vertebral da Internet *(backbone*), de relé rádio, computadores, e, a infraestrutura física da Internet que constitui um conjunto de equipamentos instalados no território, submetido às limitações da geografia física e política, que permitem construir, modificar ou destruir, ligar ou desligar a rede. Os autores Robine e Salamatian (2014) mostram a importância e os desafios estratégicos dessa infraestrutura, visto que é geolocalizável. Por sua parte, Morenkova (2014) evoca, à luz das recentes revelações de Edward Snowden, ex- analista do Departamento de Inteligência dos Estados Unidos da América, quem aborda a independência das infraestruturas informáticas russa como uma condição *sine qua non* da segurança nacional. A infraestrutura física foi concebida como uma perspectiva de abertura e circulação de fluxos informacionais, sem qualquer segurança integrada. Foi neste sentido que um dos países fundadores da Internet, Pouzin (2013, p. 23), estima que, para "segurar a Internet, deve reconstruí-la partindo da base";

b) A segunda camada é a infraestrutura **lógica**. Ela inclui todos os serviços que permitem a transmissão de dados entre dois pontos da rede e, assim, enviar e receber informações, formatadas em pequenos pacotes de dados do remetente para o destinatário. A arquitetura lógica, se baseia sobre uma harmonização fundamental, uma linguagem comum que permite que todos os computadores do mundo se comunicarem uns com os outros, sob o Protocolo da Internet (TCP / IP). Esses serviços são o roteamento (escolha de uma via pela qual os pacotes de dados viajam entre duas redes), a nomeação (nome que identifica os elementos da rede ou usuários) ou, também, o endereçamento (que transforma a série de números que representam endereços em palavras inteligíveis para os usuários). Porém, alguns aspectos podem ser geolocalizados ou não, dependendo de determinados desafios técnicos (caminhos emprestados, nomes de domínio, endereços IP...). As discussões e reivindicações em torno desta questão se abordaram na Cúpula Mundial da Sociedade da Informação de 2003 onde houve acaloradas discussões, por causa do forte controle simbólico exercido pelos Estados

Unidos pelo poder decisório do Departamento de Comércio (ICANN), o que traduz a sua hegemonia ciberespacial (RABOY e LANDRY, 2004);

a) A terceira camada é a **camada de aplicação**, composta por programas informáticos permitindo que todos possam utilizar a Internet sem conhecimento profundo da programação de computadores (*web*, e-mail, redes sociais, motores de pesquisa, etc.). As recentes revelações de Snowden demonstram a problemática do sucesso mundial dos programas informáticos de algumas grandes empresas (Google, Facebook, Amazon, etc.), às quais os usuários confiam seus dados privados e são explorados engenhosamente pelas equipes de marketing ou serviços de inteligência dos países. O que Grumbach e Frénot (2013) consideram como o novo ouro negro da economia. Os dados não se evaporam nas nuvens, mas são armazenados em servidores geridos por entidades privadas ou públicas, e muitas vezes fora do território da entidade pertencente;

b) A quarta camada é a da **informação** e **interação social**, também chamada, às vezes, de camada cognitiva ou semântica. É a dos usuários, das discussões e intercâmbios em tempo real no mundo todo, o mais difícil de capturar (em certas medidas) e representar geograficamente. Esta não é, contudo a menos relevante do ponto de vista geopolítico, quando se chega a determinar, por exemplo, que são os países mais "amigáveis" no Facebook, em que línguas estão disponíveis os conteúdos em algumas regiões do planeta, onde ou como atingem as revoltas nas redes sociais ou as campanhas de desinformação contra um governo ou uma instituição.

Também na literatura cientifica, o autor Lévy (1998, p.104) pôs ênfase na conversão deste espaço em um terreno de conflitos geopolíticos. Na concepção do autor, o ciberespaço designa “O universo das redes digitais como lugar de encontros e de aventuras, terreno de conflitos mundiais, nova fronteira econômica e cultural [...]”.

Os conflitos ocorridos no ciberespaço se caracterizam pela sua grande diversidade, sejam técnicas utilizadas, os objetivos ou os seus autores. Assim, para abordar os atos e atividades fraudulentas relativas ao ciberespaço, o autor Romani (2008) refere-se a uma guerra informática para caracterizar as ações destinadas a paralisar os sistemas de informação de uma instituição ou um negócio, ou para desviar ou distorcer os dados. De acordo com Romani (2008, p. 11), existem três modos principais de guerra de informação:

a) A **guerra contra a informação**, que ataca a integridade dos sistemas informáticos para perturbar ou interromper a seu funcionamento;
b) A **guerra pela informação**, que visa penetrar as redes para recuperar informações que circulam ou são armazenados lá;
c) A **guerra para a informação**, que usa o vetor informático para fins de propaganda, desinformação ou ação política.

Por isso, no advento da Sociedade da Informação, em que as tecnologias da informação e comunicação, exercem um papel preponderante nas infraestruturas das nações e na interação entre elas; as infraestruturas de informação tentam serem críticas, posto que possam sofrer incidentes de diferentes proporções que desemboquem, por exemplo, em desfuncionalidades. Se elas param, a Sociedade da Informação também para, com graves consequências sobre os ***ativos de informação*** da sociedade real (KEMPF, 2012).

Diante este papel central dos sistemas de informação e comunicação e a extrema dependência das nossas sociedades, o ciberespaço tende aumentar cada vez mais seu território com o desenvolvimento de Novas Tecnologias de Informação e Telecomunicações (NTIC), e sua crescente interligação e a generalização da sua utilização na vida diária dos Estados. Por isso, o aperfeiçoamento da proteção e defesa dos sistemas de informação é uma questão importante questão de segurança nacional onde a constante intervenção do Estado, blocos de interesses, organizações, etc., revê-se segundo sua necessidade.

2. POLÍTICAS INTERNACIONAIS DO CIBERESPAÇO

Devido à natureza global do ciberespaço e a utilização mais ativa das tecnologias da informação e comunicações (TIC), a problemática do ciberespaço se revê de caráter universal e transnacional, o qual, afeta tanto aos países, a sociedade global como aos indivíduos. Partindo da premissa de que o problema da segurança da informação não seria resolvido pelos esforços de um Estado ou um grupo de Estados, encarar os incidentes cibernéticos parece exigir esforços conjuntos da comunidade internacional como um todo. Por isso, é pertinente abordar brevemente algumas políticas globais com fim de promover a segurança cibernética.

2.1 A Organização das Nações Unidas (ONU)

A questão da segurança da informação tem sido abordada na agenda da ONU desde que a Federação da Rússia, em 1998, introduziu pela primeira vez um projeto de resolução na Primeira Comissão da Assembleia Geral da ONU. Esta resolução foi aprovada sem votação (A/RES / 53/70) e continuou até ser uma proposta mais detalhada, a pesar de que os seus conteúdos fossem conflitantes e, provavelmente, inexequíveis (UN, 2011). A este propósito, Rojas (2013, p. 274) relata que:

> Esses projetos de resolução tornaram-se um exercício anual de frustração: a iniciativa russa, durante muitos anos, foi rejeitada por alguns países ocidentais, mas ainda tem o mérito incontestável de manter vivo o argumento de que era necessário um importante esforço legislativo.

A resolução 66/24, na sua seção 3, convida todos os Estados-Membros, levar em conta as avaliações e recomendações contidas no relatório do Grupo de Peritos Governamentais sobre a evolução no domínio da informação e das telecomunicações no contexto da segurança

internacional (UN, 2011, p. 18); e, segue comunicando ao Secretário-Geral as suas opiniões e comentários sobre:

a) A avaliação global dos problemas de segurança da informação;
b) As medidas tomadas a nível nacional para reforçar a segurança da informação e contribuir para a cooperação internacional nesta área;
c) O conteúdo dos conceitos mencionados no parágrafo 2 da resolução;
d) As medidas que a comunidade internacional poderia adotar para fortalecer a segurança da informação à escala mundial.

Em um marco global, a Organização das Nações Unidas (ONU) adotou vários documentos com respeito às Tecnologias da Informação e Comunicação e os aspectos relacionados à segurança. Neste contexto, a primeira Comissão de Desarmamento e Segurança da Assembleia Geral da ONU adotou várias resoluções internacionais e constituiu um grupo de peritos governamentais (ROJAS, 2013). Este grupo apresentou um relatório em 2010 que promove a concertação entre os Estados sobre as normas eventuais relativas ao uso das Tecnologias da Informação e Comunicação para adotar medidas de confiança, estabilidade e redução dos riscos, a troca de informações sobre as legislações e estratégias nacionais de segurança relativas às Tecnologias da Informação e Comunicação, e, identifica os recursos para os países menos desenvolvidos para reforçar as suas capacidades.

Na sua Resolução 65/41 (UN, 2011), aprovada em novembro de 2011, a Assembleia Geral das Nações Unidas decidiu retomar o trabalho do grupo de Peritos Governamentais em 2012. Estas decisões devem fundamentar-se sobre a definição de medidas de confiança para fortalecer a segurança ou a busca de um consenso sobre padrões de comportamento no ciberespaço. Para isso, conferem-se poderes a várias Organizações das Nações Unidas no cumprimento dessa meta.

3.2 União Internacional das Telecomunicações (UIT)

Cabe lembrar-se que a União Internacional das Telecomunicações (UIT), organização especializada das Nações Unidas, cujo objetivo principal é a padronização das telecomunicações, tem organizado conjuntamente com a Assembleia Geral das Nações Unidas, a Cúpula Mundial sobre a Sociedade da Informação, em que teve duas sessões realizadas em 2003 e 2005, em que foi discutida a questão da governança da Internet.

A UIT trabalha para estabelecer um marco internacional a fim de promover a segurança cibernética, através de um “Programa Global de Segurança Cibernética” e, tem criado em 2008, um grupo de peritos de alto nível encarregado de propor uma estratégia em longo prazo, englobando medidas legais, técnicas com fim de remediar as falhas dos produtos de software; bem como a prevenção e a detecção de ataques informáticos e a gestão de crises (UIT, 2009).

No Fórum da Cumbe Mundial sobre a Sociedade da Informação (CMSI), em 2011, foi realizado um debate de alto nível sobre a "Criação de confiança e segurança no ciberespaço". A União Internacional das Telecomunicações, o Departamento de Assuntos Econômicos e Sociais e a União Interparlamentaria organizaram o IV Fórum Parlamentário sobre o tema “O triplo desafio da segurança cibernética: informação, cidadãos e infraestrutura” (ITU, 2011). O Conselho Econômico e Social, o Departamento de Assuntos Econômicos e Sociais e a UIT organizaram uma reunião especial sobre cibersegurança e desenvolvimento.

A agenda sobre a Cibersegurança Global, introduzida pela UIT em 2007, continua fornecendo um marco de resposta internacional aos desafios crescentes. Desde 2008, a UIT colabora com a “Aliança Internacional Multilateral contra as Ciberameaças (IMPACT)” e estabeleceu a primeira aliança verdadeiramente global entre múltiplos interessados e os setores público e privado para combatê-las (UIT, 2008). Segundo Schjølberg (2008), a UIT e a IMPACT realizaram em uma trintena de países menos adiantados nos programas de formação conjunta sobre a criação de equipes nacionais encarregados dos incidentes informáticos, e, atualmente, 10 países estão criando as suas equipes nacionais.

Com a publicação do manual o “Cibercrime: Uma guia para os países em desenvolvimento” (UIT, 2009), a UIT e o Escritório das Nações Unidas sobre Drogas e Crime assinaram um memorando de entendimento para colaborar globalmente, ajudando os Estados-Membros a reduzir os riscos de cibercrime. De fato, foi lançada, em 2011, a “National Cybersecurity Strategy Guide” (Guia Estratégica de Segurança Cibernética Nacional) para ajudar os governos a desenvolverem as suas estratégias e respostas nacionais (UIT, 2011).

Sob a liderança de seu Secretário-Geral, a UIT pretendeu reforçar seu papel em termo de segurança cibernética, em particular na perspectiva de uma revisão do Regulamento das Telecomunicações Internacionais, em novembro 2012. O Secretário-Geral da UIT já havia mencionado, em 2010, a ideia de um tratado internacional, proibindo a ciberguerra. De acordo com Bockel (2012, p. 55), esta vontade da UIT é apoiada pela China e Rússia, que desejam usar este espaço como um dos vetores da sua abordagem da segurança cibernética, bem como pela maioria dos países em desenvolvimento.

Em contraste, alguns grandes países ocidentais se opuseram à ideia de reconhecer uma base juridicamente vinculativa ao trabalho da UIT sobre a segurança cibernética (BOCKEL, 2012). No entanto, a UIT aceitou desempenhar um papel útil no desenvolvimento de capacidades nacionais (criação de CERT, estratégias de negócios, etc.), particularmente para os países em desenvolvimento.

3.3 Organizações para a Cooperação e Desenvolvimento Econômico (OCDE)

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) é um órgão intergovernamental do qual pertencem 34 países, entre eles México e Chile da América Latina. Essa agência está autorizada para discutir políticas públicas, procurar soluções para problemas comuns entre os membros, identificar as melhores práticas e coordenar as políticas nacionais e internacionais em diversos setores, incluindo a área das Tecnologias de Informação e Comunicação.

A OCDE também está preocupada, sob a perspectiva econômica, dos ataques informáticos em vista às empresas e seu impacto sobre a economia. De acordo com Bockel (2012), a OCDE publicou, em 1992, as diretrizes relativas à segurança dos sistemas de informação, que foram atualizadas em 2001, e, daí vários documentos foram publicados, principalmente sobre a proteção das Infraestruturas críticas de informação.

Durante a reunião Ministerial sobre o "Futuro da Economia da Internet", realizada na cidade de Seul, na Coréia, em 17 e 18 de junho de 2008, se realizou um painel de discussão intitulado: "Fortalecimento da confiança", onde foram tratados alguns aspectos sobre o cibercrime e roubo de identidade nos países-membros. Assim, um comitê de segurança cibernética e um grupo de trabalho dedicado à cibersegurança foram formados no seio da OCDE e as funções deste grupo incluem a elaboração de uma lista de medidas de confiança e segurança para o ciberespaço. No entanto, de um olhar geopolítico, esse discurso de confiança tem tido devido:

> À vontade dos Estados Unidos de converter essa agência em uma verdadeira “maquina de fabricação de confiança” que desempenhou um papel importante durante a "guerra fria", pretendendo estabelecer medidas de confiança no ciberespaço, especialmente com Rússia. (BOCKEL, 2012, p. 56)

De fato, a “Declaração de Seul sobre o Futuro da Economia da Internet” (OECD, 2008, p. 7-8) que foi o resultado da reunião ministerial incluiu as seguintes recomendações sobre a segurança e o cibercrime, todas destinadas a “Fortalecer a confiança e segurança”, mediante políticas que:

a. Protejam as infraestruturas de informações críticas contra os riscos de segurança a nível nacional e internacional;
b. Reduzam as atividades maliciosas online, através do reforço da cooperação nacional e internacional entre todas as comunidades dos participantes em seu caminho para uma prevenção eficaz, proteção, compartilhamento de informações e resposta;
c. Promovam a investigação para responder às ameaças de segurança emergentes;
d. Reforcem a cooperação transfronteiriça entre os governos e as autoridades executoras de legislação nas áreas de melhoria à cibersegurança, assim como na luta contra o spam, e proteção da privacidade, etc.

Em junho de 2015, a Direção da "Ciência Tecnologia e Inovação" da OCDE publicou o "Projeto de Recomendação do Conselho sobre a gestão de riscos de segurança digital para a prosperidade econômica e social" (OCDE, 2015), no qual é estabelecida uma série de princípios destinados a complementar os processos de segurança digital de gestão de risco. O documento determina que as "partes interessadas" são os governos, organizações públicas e privadas, indivíduos que se desenvolvem no ambiente digital a totalidade ou parte das suas atividades econômicas e sociais. Segundo a Comissão de Regulação das Comunicações da Republica de Colômbia: "este documento consagra, para as partes interessadas, os seguintes princípios gerais como: conhecimento, habilidade, empoderamento, responsabilidade, respeito dos direitos humanos e os valores fundamentais e cooperação".(CRC, 2015, p. 46).

No entanto, os esforços concertados entre os Estados-Membros levaram encarar as diversas dimensões dos cibercrimes atuais. Bockel (2012), evocou a falta de experiência da OCDE com respeito à cibersegurança. De fato, ele afirma que: "Esta organização, no entanto deveria permanecer um simples fórum de intercâmbio entre os Estados-Membros por falta de verdadeira perícia sobre a cibersegurança". (BOCKEL, 2012, p. 57). Por outro lado, o documento de 2014 do Ministério de Defesa da Espanha sobre a ciberestratégia evidenciou um dilema causado pela diversidade de perspectiva vinculada à segurança e defesa dos Estados-Membros. Dito documento relata que:

> Enquanto a maioria das estratégias nacionais destinadas a abordar a segurança cibernética de uma perspectiva à segurança e defesa dos Estados, a orientação da OCDE tem sido essencialmente coordenar as iniciativas para aumentar o nível global da segurança cibernética, embora que só possamos aumentar as vantagens competitivas dos estados na nova economia. Dada esta ideia e, posto que muitos países se foquem em articular suas estratégias nacionais de segurança cibernética, a OCDE define como objetivo político fundamental do reforço das capacidades e do setor da indústria nacional no domínio da segurança cibernética. (MD, 2014, p. 84).

3. CIBERESTRATÉGIA DA UNIÃO EUROPÉIA

A União Europeia aprovou em Dezembro de 2002, a "Estratégia Europeia de Segurança (EES)" onde planejava uma Europa segura num mundo melhor. Esse documento (UNIÓN EUROPEA, 2013), levou em consideração o contexto de segurança com os desafios globais e as principais ameaças. Este contexto de segurança, produto do fim da guerra fria, caracteriza-se por uma crescente abertura das fronteiras que ligam indissoluvelmente os aspectos internos e externos de segurança. Tem havido um desenvolvimento tecnológico que aumentou a dependência da Europa em infraestrutura interconectada em áreas como os transportes, energia e informação, aumentando assim a sua vulnerabilidade.

Na revisão da EES, em dezembro 2008, o chamado "Relatório Solana" já apareceu com novas ameaças e riscos, a segurança dos sistemas de informação. Como um dos novos desafios globais e principais ameaças, se notificou o termo de "Segurança Cibernética":

> As economias modernas dependem em grande medida das infraestruturas vitais, como transportes, comunicações e fornecimento da energia, e também a Internet. A estratégia da UE para uma "Sociedade da Informação" segura na Europa, adotada em 2006, faz referência ao crime causado na Internet. No entanto, os ataques contra sistemas privados ou governamentais de TI nos Estados-Membros da UE têm dado uma nova dimensão a este problema, como uma nova arma econômica, política e militar em potencial. Deve-se continuar trabalhando neste campo para explorar uma abordagem global da UE, conscientizando as pessoas e intensificando a cooperação internacional. (UNIÓN EUROPEA , 2008, p. 5).

Assim, em março de 2010, se aprovou a estratégia de segurança interna da UE que se estende a vários setores para encarar os incidentes cibernéticos graves. Entre as ameaças definidas, esta estratégia inclui-se a cibercriminalidade, que "Representa uma ameaça mundial, técnica, transfronteiriça e anônima para os nossos sistemas de informação e, por isso mesmo, levanta inúmeros desafios suplementares às autoridades". (UNIÓN EUROPEA, 2010a, p.14).

Europa, com a sua Política Comum de Segurança e Defesa de 1999, tem desenvolvido programas e estruturas de defesa, como por exemplo, o órgão unitário para proteger a cada um dos seus membros contra os riscos e ameaças. As iniciativas de segurança mais relevantes destacam-se:

a) A criação da ENISA (Agencia Europeia para a Segurança das Redes e da Informação), em 2004, outorga consultoria para a Comissão e os Estados-Membros em matéria de segurança e produtos de TI (UNIÓN EUROPEA, 2009);

b) O programa para a Proteção das Infraestruturas Críticas (PEPIC), aprovado em 2004;

c) A proteção da Europa contra os ciberataques e as perturbações em grande escala, melhorar a preparação, a segurança e a resiliência;

d) Rumo a uma política geral de luta contra a cibercriminalidade (UNIÓN EUROPEA, 2007);

e) A Agenda Digital Europeia (UNIÓN EUROPEA, 2010b): com fim de estruturar suas principais ações em torno da necessidade de encarar sistematicamente os sete seguintes aspectos problemáticos: 1) Fragmentação dos mercados digitais; 2) Falta de interoperabilidade; 3) Aumento da cibercriminalidade e risco de escassa de confiança nas redes; 4) Falta de investimentos nas redes; 5) Insuficiência dos esforços de investigação e inovação; 6) Carências na alfabetização e capacitação digital; 7) Perda de oportunidades para enfrentar os desafios sociais.

Esta agenda fornece uma visão dos problemas e das oportunidades atuais e previsíveis; e, evoluirá em função da experiência e das rápidas mudanças da tecnologia e sociedade. Por outro lado, ela levanta um conjunto de iniciativas legislativas propostas no marco da Agenda Digital e são distribuídas nos seguintes pontos: a) um mercado único digital dinâmico; b) interoperabilidade e normas; c) confiança e segurança; d) o acesso rápido e ultrarrápido à

Internet; e) fomentar a alfabetização, capacitação e inclusão digital; f) benefícios que favorecem as TIC para a sociedade da EU (UNIÓN EUROPEA, 2010b).

Em quanto à Internet, a nova situação provocada pelas revelações de Snowden sobre os programas de vigilância em massa na Internet pelos Estados Unidos cria uma oportunidade para a Europa se tornar o arquiteto de um acordo transatlântico que estabeleceria os princípios básicos do desenvolvimento da Internet fundamentado nos respeitos dos valores democráticos. Nesta perspectiva, o inventor da web, o britânico Tim Berners-Lee, tem afirmado que seja criada uma Constituição mundial para a Internet (BERNERS-LEE, 2014).

De acordo com Benhamou (2014), desta proposta, seria conveniente adicionar uma seção que proibiria os Estados a tomar medidas que podem afetar o funcionamento da rede para todos os seus usuários. Também a criação de um acordo transatlântico que estabeleceria uma exigibilidade jurídica internacional às ações tecnológicas dos Estados que obstaculizam o bom funcionamento e a segurança da rede. Posteriormente, poder-se-ia ampliar por outros regimes democráticos para evitar novas crises de confiança que enfraquecem a arquitetura global da Internet.

Como ressaltou o recente relatório do Senado da União Europeia sobre a governança global da Internet, o desenvolvimento de um tratado transatlântico sobre a governança da Internet revê de fato um caráter fundamental para os países da União Europeia:

> A União Europeia tem que fazer ouvir a sua voz no atual debate sobre a futura governança da Internet. Mas é certo que a sua credibilidade será ainda mais forte do que ela tem, internamente, replanejado o seu futuro digital para conquistar um peso real no ciberespaço. (MORIN-DESAILLY, 2014, p. 149).

Vários passos têm sido dados no marco europeu, mas ainda precisam convergir os esforços, sobretudo, para conseguir a independência tecnológica. No núcleo do desenvolvimento de uma Política Europeia de segurança cibernética, se encontraria o desenvolvimento integral de uma Estratégia Europeia de cibersegurança. Para Alcançar tal meta, o Parlamento Europeu propôs uma resolução sobre a aplicação de uma Estratégia Comum de Segurança e Defesa. Outras propostas incluem a criação de um conselho, de um coordenador ou de uma agência europeia de cibersegurança.

3.1 Panorama ciberespacial da América Latina e do Caribe

De acordo com um estudo da Organização dos Estados Americanos (OEA, 2013), o conhecimento disponível sobre o panorama geral das ameaças cibernéticas e respostas dos governos da América Latina e o Caribe é incompleto. Este estudo relata que: “Todo que se sabe sobre o cenário das ameaças cibernéticas na região é baseada em reportagens esporádicas sem fundamentos de bases sólidas”. (OEA, 2013, p. 1).

Portanto, em 2012, os governos observaram um aumento geral na frequência de incidentes cibernéticos em relação a 2011, mesmo que os dados quantitativos definitivos estavam incompletos ou não estavam disponíveis. De acordo com o relatório da OEA (2013, p.3):

> O aumento mínimo de incidentes cibernéticos avaliados durante o período de 2011-2012 foi registrado por um governo foi entre 8% e 12%; enquanto no extremo superior, outros dois países registraram um aumento de 40%. A maioria dos governos citou o aumento em algum ponto dentro desta escala, embora seja interessante notar que vários relataram que, em geral, foram detectados menos incidentes.

Nesse sentido, Martin (2015) argumenta que essa disparidade perceptível em porcentagem de incidentes cibernéticos entre os Estados deve-se à disparidade de usuários de Internet nos países latino-americanos. Esta realidade constitui um elemento importante do contexto a ser tido em conta na avaliação dos riscos cibernéticos. Assim, o autor afirma que:

> Poder-se-ia facilmente dizer que os países menos conectados experimentam um risco estatisticamente menor em seu escopo onde a penetração da Internet já está bastante avançada pelo simples efeito de um menor número de vitimas potencias. No entanto, nos países menos conectados, os grandes ausentes são os usuários individuais, especialmente aqueles que estão localizados na periferia da rede de infraestruturas de comunicação, como zonas rurais e áreas de extrema pobreza. Tem como efeito lógico uma sob-representação de ataques direcionados contra as instituições públicas e privadas. Ao contrario, nos países mais conectados, a população está diretamente envolvida nas problemáticas de segurança e pode ter um efeito sobre as ações a serem realizadas pelo seu comportamento individual e da expressão de uma reivindicação política. (MARTIN, 2015, p. 5).

Por outro lado, o documento da OEA (2013) relata que o ativismo, ou cibercrime por motivos políticos, recebeu grande atenção da mídia em 2012, e as informações fornecidas pelos Estados-Membros mostram que esta forma de incidentes cibernéticos está aumentando verdadeiramente na região. Segundo a OEA (2013, p.4), dois países reportaram:

> Campanhas de ciberataques coordenados como resposta a iniciativas legislativas destinadas a reforçar a aplicação das leis de direitos autorais e reformar códigos tributários. Em ambos os casos, se aproximava a ratificação dos respectivos projetos de lei; os fóruns de hackers estavam saturados com planos para realizar ataques cibernéticos de grande escala contra as infraestruturas governamentais no caso que a legislação não seja vetada.

Apesar de sua maior visibilidade, o ativismo não substituiu os benefícios pecuniários como a principal motivação que subjaza a invasão e o uso ilícito da internet na região. Os hackers continuaram procurando dados pessoais e financeiros e alimentando os mercados negros online no mundo. No entanto, é impossível medir com precisão,

> O impacto quantitativo e perdas econômicas causadas pelo roubo de informação na América e no Caribe em 2012. O número é extraordinariamente elevado, provavelmente maior do que as perdas causadas por qualquer forma de crime, incluindo o tráfico de drogas. (OEA 2013, p.5).

O autor Martin (2015), preocupado pelas novas tendências de incidentes cibernéticos contra as nossas infraestruturas, aquelas que implicam as principais vulnerabilidades na disponibilidade de energia, serviços de comunicação, recursos necessários no processo produtivo, evidenciou uma falta de consciência e de interesse nas questões de cibersegurança. De fato, ele afirma que "Enquanto as infraestruturas dos países latino-americanos apresentam inúmeras falhas de segurança, algumas nem sequer estão protegidas por uma simples senha". (OEA, 2015 citado por MARTIN, 2015, p.7).

Cabe mencionar, também, que as agências latino-americanas de inteligência carecem de pessoal com alto nível de conhecimento, experiência e compreensão do cenário de ameaças *online*. Na verdade, alguns países têm trabalhado para criar unidades contra os cibercrimes. No entanto, estas unidades são frequentemente focadas em investigações forenses digitais (encontrar a agulha no palheiro), provas digitais (descoberta, preservação, gestão e apresentação) e antipirataria dos direitos de autor. Assim, argumenta-se que:

> As autoridades nacionais tropeçam regularmente ao desenvolvimento das capacidades do pessoal responsável pela segurança cibernética e crime cibernético, por exemplo, a participação de técnicos de diversas instituições públicas em cursos sobre segurança da informação, gestão de incidentes, o trabalho redes sociais, computação forense e pirataria legítima. (OEA, 2014, p. 91).

Por outra parte, a ICANN, em seu relatório sobre o panorama do ciberespaço na América Latina e o Caribe apontou à problemática da antiguidade dos equipamentos das Infraestruturas de informação. Dito relatório citado pela OEA (2014) evoca:

> A problemática do roteamento, uma das funções mais importantes com respeito à operacionalização da Internet [...]. Por entanto, na America Latina, o sistema de roteamento é baseado em tecnologias que, essencialmente, não foram alteradas por mais de 15 anos. (OEA, 2014, p. 93).

Lemarchand e Sidney (2014), na sua abordagem da cibersegurança nos países emergentes e América Latina, introduziram o conceito de "ciberparaíso" e "paraíso digital", ou melhor em inglês, *data heaven*, referindo-se às verdadeiras bases do cibercrime internacional que, como tal, constituem um obstáculo importante para a luta contra a cibercriminalidade. Esses paraísos digitais são definidos como lugares onde um criminoso pode agir ou alojar servidores e conteúdos ilegais com impunidade. Segundo os autores, esses paraísos são constituídos por:

> Estados ou atores do setor privado que fornecem estruturas, alojamento ou leis laxistas; por exemplo, eles garantem seus clientes de não dar seguimento à nenhum pedido de cooperação internacional, e no jeito dos paraísos fiscais, promover a proliferação de atos cibercriminais à imunidade judicial, dificultando enormemente os esforços da comunidade internacional. (LEMARCHAND; SIDNEY, 2014, p. 22).

Alguns autores sustentam que o ambiente cibernético da América Latina e do Caribe favorece o desenvolvimento dos incidentes cibernéticos. Assim, parece óbvio que a oportunidade econômica e a falta de legislações catalisam a preferência da nossa região pela

cibercriminalidade, o que dificulta, ainda mais, a abordagem dos atores regulamentadores. Desta maneira, Goncharov (2012, p.13) evidenciou esse fato, quando afirma que "Em contraste com a preferência por servidores pagos e de proxy que manifestam os criminosos na Europa Oriental, os da América Latina preferem usar serviços de hospedagem gratuita".

Também cabe ressaltar que, em contraste com os padrões globais, os criminosos cibernéticos na América usam serviços comuns de transferência de dinheiro para pagar os bens e serviços dos cibercriminosos. Posto que isso pudesse conduzir a sua identificação pelas autoridades; assim,

> Os cibercriminosos contratam "mulas" para realizar as transações. Além disso, sistemas como Webmoney estão sendo usados amplamente, isso evidencia a crescente colaboração internacional entre os cibercriminosos que operam na América Latina e Europa Oriental. (OEA, 2013, p. 17).

Diante este crescimento multidimensional dos incidentes cibernéticos na América Latina e o Caribe, as partes implicadas precisam desenvolver estratégias para poder encarar ditos incidentes em suas diversas formas. E, isso requer a multiplicação de esforços e convergência dos atores tanto nacionais como regionais pela segurança do nosso ciberespaço.

4. CONSIDERAÇÕES FINAIS

De acordo às considerações anteriores, podemos ressaltar que a principal característica que tem contribuído a esse desenvolvimento e dependência do ciberespaço é o tratamento da informação e a abrangência das Tecnologias da Informação e Comunicação. Na chamada "sociedade da informação", ou cibersociedade (JOYANES, 1997), a premissa é que a informação em si possui um valor susceptível de gerar poder (político, econômico, social, etc.). Quanto maior a eficiência com que seja tratada e manejada, maior seriam os seus benefícios. Assim, o ciberespaço tem experimentado um enorme e rápido desenvolvimento, traduzindo-se como um novo modelo de dependência na sociedade de hoje, o que contrasta com o menor e lento progresso em matéria de segurança cibernética. Por esta razão, se converte também em um campo a ser regulamentado pelos atores que optam operar na cibersociedade.

As Políticas globais de Informação do Ciberespaço se destinam a responder às novas preocupações de segurança na Cibersociedade; no entanto, os Estados apresentam uma linha comum de defesa cibernética; às vezes, estão alinhados a uma grande potência como, por exemplo; os Estados Unidos. Contudo, as Políticas globais de Informação, baseadas sobre uma cooperação global ou regional, exibem ambições dispares.

As políticas de informação planejadas ao nível nacional para encarar as ameaças do ciberespaço se fundamentam sobre uma cooperação internacional, embora que no ciberespaço, estejamos diante ameaças que contornam as fronteiras. Porém, em nome da segurança nacional, as políticas globais e cooperativas evoluem em um ambiente de

desconfiança. Como se preconiza sempre que em matérias de ciberestratégias não há amigos; às vezes, muitos Estados privilegiam as cooperações bilaterais com os seus aliados próximos e relutam em levantar estas questões num marco multilateral.

Na análise do cenário ciberespacial da região Latino-Americana e o Caribe, percebe-se que, além dos esforços consentidos pelos diversos atores da nossa região, a necessidade de profissionais altamente capacitados que podem proteger as redes, diagnosticar as intrusões e gerenciar eficazmente os incidentes cibernéticos quando eles ocorrem. Esses problemas se destacam mais nas regiões com baixas porcentagens de programas de capacitação.

As literaturas deduzem que a dependência da nossa região dos países tecnologicamente desenvolvidos, do capital privado externo, a falta de consciência sobre o valor da informação, de capital humano, de investimento, de legislações idôneas e a antiguidade dos equipamentos das Infraestruturas de informação são fatores que criam obstáculos à segurança cibernética. Por isso, precisamos unir esforços para desenvolver e criar Políticas de Informação para o desenvolvimento de uma infraestrutura e infroestrutura ideal para a região, em conformidade à revolução digital e tecnológica.

REFERÊNCIAS

BENHAMOU, Bernard. Organiser l'architecture de l'Internet. **France-Diplomatie**, n° 4, Avril, 2014. Disponível em: <http://www.diplomatie.gouv.fr/IMG/pdf/OrganiserlarchitecturedelinternetBernardBenhamou-2.pdf>. Acesso em: 24 Jun. 2017.

BERNERS-LEE, Tim. **An online Magna Carta: Berners-Lee calls for bill of rights for web**. (The Guardian, 12/03/2014). Disponível em: <https://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web>. Acesso em: 23 Jul. 2017.

BOCKEL, Jean-Marie. Rapport D´Information. Sénat - Session extraordinaire de 2011-2012. **Enregistré à la Présidence du Sénat** le 18 juillet 2012. Disponível em: <https://www.senat.fr/rap/r11-681/r11-6811.pdf>. Acesso em: 24 Jul. 2017.

BRUNO, Vitorio. **Arquitetura de redes de computadores**. Universidade Federal de Santa Catarina. Departamento de Informática e de Estatística. Florianópolis, SC, 2000. Disponível em: < http://www.joinville.udesc.br/portal/professores/flavio/materiais/Redes.pdf>. Acesso em: 22 Jul. 2017.

CRC. Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad. **Documento de análisis y consulta**. Coordinación Relaciones de Gobierno y Asesoría. Todos por un nuevo país. Comisión de Comunicaciones. Colombia, Julio de 2015. pp, 4 – 84.

DOUZET, Frédérick. La géopolitique pour comprendre le cyberespace. **La Découverte**. 2014. pp 3 – 21. Disponível em: < https://www.herodote.org/IMG/pdf/Douzet.pdf>. Acesso em: 20 Jul. 2017.

GÓMEZ, Ángel. **El ciberespacio como escenario de conflictos**. Identificación de las amenazas. Centro Superior de Estudios de la Defensa Nacional: Febrero, 2012. pp. 169 – 203. Disponível em: <http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf>. Acesso em: 28 Abr. 2017.

GONCHAROV, Max. **Russian underground 101.** Trend Micro Incorporated Research Paper 2012.

GRUMBACH, Stéphane ; FRENOT, Stéphane. Les données, puissance du futur. **Le Monde Diplomatique**. France, nº 3, Janvier 2013. Disponível em: <http://www.lemonde.fr/idees/article/2013/01/07/les-donnees-puissance-du-futur_1813693_3232.html>. Acesso em: 28 Jun. 2017.

ITU. **Repport-fourth parliamentary forum on shaping the information society.** The triple challenge of cyber-security: information, citizensand infrastructure". ILO Conference Center International Labour Organization Geneva, Switzerland, 2011. Disponível em: <http://www.itu.int/net/wsis/implementation/2011/forum/inc/Documents/WSISForum2011OutcomeDocument.pdf>. Acesso em: 10 Mar. 2017.

JOYANES, Luis Aguilar. **Cibersociedad:** los retos sociales ante un nuevo mundo digital. McGraw-Hill. España, 1997.

KEMPF, Olivier. **Introduction à la Cyberstratégie**. Paris, Broché, 2012.

LEMARCHAND, Hugo; SIDNEY, Barbara. **Cybersécurité des pays émergents. États des Lieux. Les notes stratégiques**. CEIS. Paris, 2014. pp. 3 – 33.

LÉVY, Pierre. L´intelligence collective. Pour une anthropologie du Cyberspace. **La Decouverte/Poche**. Paris, 1998.

MARTIN, P. Edouard. Inseguridad cibernética en América Latina: líneas de reflexión para la evaluación de riesgos". **Documentos de Opinión**. Ieee. es. 2015.

M. D. Documentos de seguridad y defensa. Estrategia de la información y seguridad en el ciberespacio. **Escuela de Altos Estudios de la Defensa.** Ministerio de Defensa. España, Junio 2014. Disponível em: < http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/060_ESTRATEGIA_DE_LA_INFORMACION_Y_SEGURIDAD_EN_EL_CIBERESPACIO.pdf > Acesso em: 30 Jul. 2017.

MONTVILOFF, Victor. **Políticas nacionales de información -** Manual sobre la formulación, aprobación, aplicación y funcionamiento de una política nacional sobre la información. Programa General de Información y UNESCO, París: Unesco, 1990. Disponível em: < http://unesdoc.unesco.org/images/0008/000869/086995sb.pdf > Acesso em: 07 Ag. 2017.

MORENKOVA, Elena. De la sécurité informationnelle à la Cybersécurité: la redéfinition de la doctrine stratégique russe. **TRIBUNE.** Université de Paris, n. 586, v2, 2014. . Disponível em: <http://www.academia.edu/10278359/_De_la_s%C3%A9curit%C3%A9_informationnelle_%

C3%A0_la_cybers%C3%A9curit%C3%A9_la_red%C3%A9finition_de_la_doctrine_strat%C3%A9gique_russe_Revue_D%C3%A9fense_Nationale_Tribune_n_586_D%C3%A9cembre_2014_pp._1-7> Acesso em: 20 Jul. 2017.

MORIN- DESAILLY, Catherine. L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne**. Repport d'information n° 696(2013-2014);** fait au nom de la MCI sur la gouvernance mondiale de l'Internet, déposé le 8 juillet 2014. Disponível em : < https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf> Acesso em: 07 Ag. 2017.

OECD. **The Seoul declaration for the future of the internet economy**. Ministerial Session. Korea, June 2008. Disponível em: <http://www.oecd.org/sti/40839436.pdf>. Acesso em: 25 Jul. 2017.

OEA. **Tendencias de seguridad cibernética en América Latina y el Caribe**. Washington: SYMANTEC, 2014. Disponível em: < https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf > Acesso em: 25 Jul. 2017.

____. **Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos**. Washington: TEND Micro, 2013. Disponível em: < http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf > Acesso em: 07 Ag. 2017.

_____. **Reporte de seguridad cibernética e infraestructura crítica**. Washington: TEND Micro, 2015. Disponível em: < https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf > Acesso em: 07 Ag. 2017.

OTTIS, Rain; LORENTS, P. **Cyberspace:** definition and implications. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2011. Disponível em: <https://www.academia.edu/16137618/3rd_International_Conference_New_Functional_Materials_and_High_Technology_NFMaHT_2015?auto=download>. Acesso em: 06 Jun. 2017.

POUZIN, Louis. L'Internet doit être refait de fond en comble. **Les Échos**, n° 21442, 24 mai 2013. Disponível em : < https://www.lesechos.fr/24/05/2013/LesEchos/21442-102-ECH_louis-pouzin-----l-internet-doit-etre-refait-de-fond-en-comble--.htm> Acesso em: 30 Jul. 2017.

RABOY, Marc; LANDRY, Normand. La communication au cœur de la gouvernance globale. **Enjeux et perspectives de la société civile au sommet de la Société de l'information**. Canada: SMSI, Département de communication, 2004. Disponível em : < http://www.lrpc.umontreal.ca/smsirapport.pdf > Acesso em: 05 Ag. 2017.

ROBINE J.; SALAMATIAN Kave. Peut-on penser une cybergéographie?. **HÉRODOTE. La Découverte**. Paris, 2014.

ROJAS, Emilio. Cooperación internacional en temas de ciberseguridad. In. **Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa:** un reto prioritario. España: Ministerio de defensa, 2013. Disponível em : < http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NE

CESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf > Acesso em: 07 Ag. 2017.

ROMANI, Roger. **Rapport D´Information. Sénat - Session extraordinaire de 2007-2008**. Annexe au procès-verbal de la séance du 8 juillet 2008. Au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense. Strasbourg, France. Disponível em: < https://www.senat.fr/rap/r07-449/r07-4491.pdf > Acesso em: 07 Ag. 2017.

SCHJØLBERG, Stein; ITU Global Cybersecurity Agenda (GCA); High-Level Experts Group (HLEG). **Report of the chairman of HLEG**. Norway: ITU, 2008. Disponível em: < https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf > Acesso em: 07 Ag. 2017.

SCHOENBERGER, Viktor; ZIEWITZ, Malte. Sciences and Technology- Law review. **Jefferson Rebuffed - The United States and the future of internet governance**. John F. Kennedy School of Government, Harvard University, The Colombia, 2006. Disponível em: < http://stlr.org/download/volumes/volume8/schoenberger.pdf > Acesso em: 26 Jul. 2017.

UIT. International Telecommunication Union, Rec. SERIES X: Data networks, open system communications and security. **Telecommunication security**. April, 2008. UIT-T X.1205

___. Recursos jurídicos contra el ciberdelito. **El ciberdelito: guía para los países en desarrollo.** Ginebra: Departamento de Políticas y Estrategias; División de Aplicaciones TIC y Ciberseguridad. Sector de Desarrollo de las Telecomunicaciones de la UIT, 2009. Disponível em: < https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf > Acesso em: 28 Jul. 2017.

UNIÓN EUROPEA. **Una Europa segura en un mundo mejor. Estrategia europea de seguridad**. Bruselas. 2013. Disponível em: < http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Ar00004>. Acesso em: 24 Jul. 2017.

UNIÓN EUROPEA. **Estratégia de segurança interna da União Europeia. Rumo a um modelo europeu de segurança.** Bélgica, 2010a. Disponível em: <http://register.consilium.europa.eu/doc/srv?l=PT&f=ST%2015670%202014%20INIT>. Acesso em: 24 Jul. 2017.

UNIÓN EUROPEA. **Uma Agenda Digital para a Europa**. Bélgica, 2010b. (Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões). Disponível em: <http://ec.europa.eu/europe2020/pdf/europe2020stocktaking_pt.pdf>. Acesso em: 21 Jul. 2017.

UNIÓN EUROPEA. **Parecer do CES Europeu sobre a Comunicação da Comissão ao Parlamento Europeu, ao Conselho. Comitê Econômico e Social Europeu e ao Comitê das Regiões**. C255/98. 22.9.2010. Comunicação COM (2009). Sec. 149. Bruxelas, 30 de Março de 2009. Disponível em: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-134-F1-PT-MAIN-PART-1.PDF>. Acesso em: 18 Abr. 2017.

 DOI 10.20396/rdbci.v15i3.8647632

UNIÓN EUROPEA. **Informe Solana. Informe sobre la aplicación de la Estrategia Europea de Seguridad**. Ofrecer seguridad en un mundo en evolución. Bruselas: UE: Diciembre del 2008. Disponível em: <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf>. Acesso em: 24 Jul. 2017.

UNIÓN EUROPEA. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões**. COM (2007) 267 final. Novembro 2007. Disponível em: < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52007DC0267>. Acesso em: 22 Jul. 2017.

VERA, G. Roberto. La sociedad de la información en México frente al uso de internet. **Revista Digital Universitaria.** Volumen 5, num. 8, UNAM, México, 2004. Disponível em: <http://www.revista.unam.mx/vol.5/num8/art50/sep_art50.pdf> Acesso em: 05 Ag. 2017.

ISSN 1678-765X
17>
9 771678 765041