UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

FACULDADE NACIONAL DE DIREITO

DANIELLE CUSNIR

A PROBLEMÁTICA DOS CIBERATAQUES EM UM CONTEXTO DE COOPERAÇÃO JURÍDICA INTERNACIONAL

Rio de Janeiro

2018

DANIELLE CUSNIR

A PROBLEMÁTICA DOS CIBERATAQUES EM UM CONTEXTO DE COOPERAÇÃO JURÍDICA INTERNACIONAL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré requisito para obtenção do grau de bacharel em Direito, sob orientação do Professor Ms. Felipe Gomes de Almeida Albuquerque.

Rio de Janeiro

2018

CIP - Catalogação na Publicação

Cusnir, Danielle

Cp

A PROBLEMÁTICA DOS CIBERATAQUES EM UM CONTEXTO DE COOPERAÇÃO JURÍDICA INTERNACIONAL / Danielle

Cusnir. -- Rio de Janeiro, 2018.

66 f.

1. Ciberataque. 2. Soberania. 3. Cooperação Jurídica Internacional. I. Gomes de Almeida Albuquerque, Felipe, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

DANIELLE CUSNIR

A PROBLEMÁTICA DOS CIBERATAQUES EM UM CONTEXTO DE COOPERAÇÃO JURÍDICA INTERNACIONAL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré requisito para obtenção do grau de bacharel em Direito, sob orientação do Professor Ms. Felipe Gomes de Almeida Albuquerque.

Data de aprovação: __/___/____.

Banca Examinadora:

_____
Orientador

_____
Membro da Banca:

_____
Membro da Branca:

Rio de Janeiro

2018

À vida, por me proporcionar a vivência de momentos tão importantes para a construção de quem eu sou hoje.

Por nunca me deixar faltar saúde e felicidade e, principalmente, por ter me guiado em um caminho de muita sorte, luz, grandes oportunidades, realizações e conquitas.

Só tenho agradecimentos a esse momento da minha vida.

"Não existe caminho para a felicidade. A felicidade é o caminho"

RESUMO

O desenvolvimento tecnológico trouxe para o mundo globalizado que vivemos hoje um grande impacto nas relações pessoais, econômicas, sociais e políticas. Servindo, muitas vezes, como suporte nas diversas áreas do conhecimento humano, a tecnologia vem sendo usada, também, como instrumento de condutas ilícitas e fraudulentas. Ao passo que as fronteiras geográficas deixam de existir, aproximando os indivíduos, esse novo ambiente vem se mostrando extremamente propício para condutas que se notam difíceis de se apurar os agentes, o tempo e o espaço em que são realizadas. Desse modo, a ideia de soberania e nação vem se transformando, de modo que os Estados carecem de apoio, um do outro, quebrando suas fronteiras físicas, no intuito de apurar condutas que, atualmente, tampouco demonstram limitação de espaço físico, seja nas ações, seja nos resultados das mesmas. Acompanhando esse panorama, o presente estudo busca analisar essa nova dimensão de ação, que não está mais restrita ao plano físico, passando a observar as condutas praticadas no plano tecnológico, especificamente os ataques cibernéticos, e avaliar desses na cooperação jurídica entre os Estados, em um esforço conjunto de atuar no espaço cibernético, para solucionar condutas que geram efeitos e resultados no plano fático e físico dos Estados. Especificamente, analisa-se no presente o histórico, as características e os elementos de um ataque cibernético e seus efeitos no âmbito social e jurídico. Superado esse ponto, serão analisados os meios de cooperação jurídica internacional dos Estados e os esforços necessários para neutralizar impactos gerados por um ciberataque. Os resultados levam a crer que ainda que os ciberataques coloquem em cheque a soberania dos Estados, ainda, os próprios Estados que detém competência para criar meios que neutralizem os ciberataques, por meio de políticas, legislações e procedimentos rápidos e eficientes de auxílio mútuo entre os Estados, para apurar, investigar, minimizar, prevenir e defender uns aos outros contra os ciberataques.

Palavras-chave: ciberataque; soberania; cooperação jurídica internacional.

ABSTRACT

The technology development brought to the globalized world that we live today a huge impact among personal, economic, social and political relationship. In one hand, technology can be used as a medium in several human knowledge, but on the other hand, it has been used, also, as a tool to practice illegal and fraudulent conducts. Whereas geographic borders are no longer existent, gathering individuals, this new technological scenario shows itself as a highly favorable place to practice conducts that are hard to discover the actor, the place and the time that the action was held or by who was realized. Therefore, the concept of sovereignty and nation are being changed, in a way that States seems to be lacking a mutual support, breaking physical borders, in order to ascertain conducts that are no longer restricted to a territorial space, nor in their action elements, neither on their result. Keeping track of the panorama, the following study intends to analyse this new dimension, unlimited by the geographical or physical space, starting to analyse the practice of conducts in the cyber space, specifically, the cyberattack, and evaluate how it can affect the legal cooperation between States in a mutual effort on acting into the cyber space, to solve actions that shows impact in the real world. It will be analysed the history and the origin of the cyberspace, the concept and the essential elements of a cyberattack and its impacts in the legal and social context. Cleared this point, it will be observed the international legal cooperation methods adopted by the States to neutralize the effects of a cyberattack. The results of the following study suggest that cyberattacks threat the sovereignty of the States. However, are the very States the ones capable to create ways to neutralize the cyberattacks through policies, legislations and procedures in a challenge to achieve the fast and efficient mutual assistance to ascertain, investigate, minimize, prevent and defend each other against a cyberattack.

Key-words: cyberattack; sovereignty; international legal cooperation.

LISTA DE ABREVIATURAS

ART - Artigo

CF – Constituição Federal

CPC – Código de Processo Civil

DSIC - Departamento de Segurança da Informação e Comunicações

EU – União Europeia

EUROPOL - Serviço de Polícia Europeu

GSCIPR – Gabinete de Segurança de Comunicação e Informação da Presdiência da República

GSI – Gabiente de Segurança Institucional

HC – Habeas Corpus

NIST - Instituto de Padrões de Tecnologia do Governo Americano

ONU – Organização das Nações Unidas

OTAN - Organização do Tratado do Atlântico Norte

PR – Presidência da República

SE - Secretário Executivo

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TJ – Tribunal de Justiça

SUMÁRIO

1. INTRODUÇÃO

No curso da história da humanidade, diversas são as formas de imposição do poder verificadas nas guerras, conquistas e combates, como, por exemplo a exploração pessoal de reféns, disputas bélicas, nucleares e, atualmente, com o desenvolvimento da tecnologia, verificamos um crescimento exponencial de combates travadas por meios tecnológicos no espaço virtual.

Logo, a tecnologia vem sendo utilizada não somente como um meio de perseguição do domínio, mas sim, como um fim em si memo. Verifica-se uma queda no uso de instrumentos bélicos para o alcance dos objetivos das nações e dos indivíduos e um aumento no uso da tecnologia como moeda de barganha ou, até, meio final de ultimato de imposição de poder.

Isso porque, o poder tecnológico, discrepante do poder bélico, não se delimita a um espaço físico. Assim, tais meios se apresentam hoje como armas que quebram fronteiras, de fácil e rápido acesso, de baixo custo, quando comparados ao poder bélico, permitindo que um resultado seja produzido, a nível global, no mesmo momento em que se verifica a própria ação.

Desse modo, conflitos fáticos e reais que antes eram disputados no plano físico, hoje podem ser travados no mundo virtual produzindo efeitos de mesma escala, ou ainda maiores, que os conflitos bélicos.

Questiona-se, portanto, até que ponto a soberania dos Estados está comprometida por meio dos conflitos virtuais e quais mecanismos podem ser utilizados pelos Estados individual e conjuntamente de modo a neutralizar os efeitos dos mesmos, independentemente da causa ou motivação que deu ensejo ao combate virtual travado.

1.1. Conflitos reais, combates virtuais

- **O "Soldado de bronze de Tallim" e o cibearataque à Estônia**

Em 22 de setembro de 1947, durante o domínio da Estônia pela União Soviética na Guerra Fria, foi construída na cidade de Tallin, na Estônia, o monumento denominado "Soldado de bronze de Tallim", representando a vitória Soviética sobre os nazistas.

Em abril de 2007, a Estônia realizou uma mudança de local de instalação da estátua, tendo transferido a mesma para o Cemitério de Defesa de Tallim. Tal decisão gerou comoção e polêmica dos russos, dentro e fora da Estônia.

No mesmo dia da mudança da obra, diversos sistemas de serviços cotidianos da Estônia começaram a ser atacados ciberneticamente, gerando impacto na rotina do país. Cabe ressaltar que, na Estônia, quase todos os serviços são conectados pela rede mundial de computadores. Como exemplo, a Estônia foi o país que deu início às votações de cargos públicos via Internet. Assim, explica-se o grande efeito dos ataques vivenciados no país em razão desse desentendimento político.

Diversos ataques se sucederam, sendo verificados ataques aos sites e sistemas governamentais, bem como a indisponibilidade de diversos serviços básicos à sociedade. Diante do contexto da situação, acredita-se que os Ciberataques tiveram origem russa. Entretanto, em face da dificuldade de se apurar fatos e evidências do combate, bem como mecanismos de punição, a questão vem sendo resolvida política e diplomaticamente.

O que importa destacar do caso é que, conflitos políticos, religiosos e econômicos que, antes, eram decididos entre os Estados por meio de guerras e represálias físicas, hoje podem ser realizadas no âmbito virtual. Não obstante a ausência de um responsável declarado pelo ataque, bem como a ausência de um respaldo estatal e/ou governamental não impede que os combates virtuais sejam relacionados a conflitos reais.

- ***"Wanna Cry"***

Outro caso de importante conhecimento foi o Ciberataque denominado "*Wanna Cry"* ocorrido em 12 de maio de 2017. O referido ataque foi classificado como o maior da história, atingindo mais de 250 mil sistemas pelo mundo em menos de 3 dias.

Diferentemente dos ataques verificados anteriormente, o vírus utilizado no Wanna Cry criptografava, automaticamente, e sequestrava arquivos dos computadores infectados e, posteriormente, pedia-se o pagamento de um valor para a devolução dos arquivos.

Como diversos serviço essenciais às populações foram afetados, a nível internacional, como redes de ensino, hospitais, instituições como tribunais, serviços de telefonia e correios, o objetivo final do ataque, que era o recebimento de pagamentos, foi sucedido, em razão da urgência que os serviços se reestabelecessem. Ademais, por inteligência do criador do ataque e infelicidade das vítimas, o pagamento podia ser realizado, mais facilmente, por meio de bitcoin.

Nessa perspectiva, os valores de recompensa se tornaram mais altos e de grande dificuldade de rastreio, razão pela qual ainda não é possível atribuir um autor ao ataque.

O que se observa, mais uma vez é que, por ausência ou insuficiência de meios definidos de cooperação e legislação entre os Estados em um âmbito de Ciberataque, o vírus foi se disseminando globalmente, de modo que a apuração dos fatos foi dificultada, bem como a tomada de medidas conjuntas entre os Estados para minimizar ou neutralizar os efeitos do Wanna Cry.

- **Netflix e Game of Thrones**

A Netflix tornou-se uma das maiores provedoras de séries e filmes a nível global com a veiculação da série Game of Thrones. Em 2017, notando o sucesso da 6ª temporada da referida série, a Netflix realizou uma grande campanha de marketing para o lançamento da 7ª temporada, que envolvia milhões de dólares entre patrocínios e produção.

Em agosto de 2017, pouco tempo antes do esperado lançamento, a plataforma do Netflix sofreu um Ciberataque, estimando-se o roubo de 1,5 terabytes de informações. Foi nesse momento que a comunidade internacional observou que as motivações de um Ciberataque estavam, de fato, se alargando. De forma que a indústria do entretenimento digital, que é capaz de angariar grandes quantias de dinheiro, também poderia ser um alvo de ataque.

O Instituto de Padrões de Tecnologia do Governo Americano (National Institute of Standards and Technology –"NIST") em articulação com Serviço de Polícia Europeu ("EUROPOL") notificaram diversos países a bloquearem o servidor e os vírus que estavam roubando os dados da Netflix.

Como, todavia, não existia um protocolo ou leis específicas para adoção de medidas de segurança contra o Ciberataque e vinculação dos países ao cumprimento da decisão, alguns optaram pelo pagamento de vultuosos valores em troca da devolução das informações e mídias digitais, enquanto outros, seguem em uma investigação até os dias de hoje para apurar o caso.

O que se torna claro, mais uma vez, é que a efetividade para a resolução ou amenização dos efeitos de um Ciberataque dependem de uma atitude conjunta em âmbito global, uma vez que os impactos se dão, também em escala mundial, tendo em vista a rapidez e o alcance dos Ciberataques.

2. ANÁLISE DE ELEMENTOS BÁSICOS

Com a constante inovação e criação dos meios tecnológicos, cada vez se torna mais desafiador gerar conceitos estáticos para situações e artefatos que estão em constante transformação e movimento.

Somado a isso, quando se trata de situações e artefatos que, além da sua dinamicidade, há o alcance a nível global, a dificuldade de uma padronização de um conceito se torna ainda mais obstaculizada. Tal fato decorre da diversidade social, econômica, religiosa e política que tais situações e artefatos são analisados e aplicados.

É nesse sentido, que se encontra o campo da tecnologia, que se expressa, no mundo físico como métodos, dispositivos e protocolos que sofrem mutações diárias, se encaixando em circunstâncias diversas a nível global e se conectam constantemente por meio da rede mundial de computadores.

Quando esse ambiente é utilizado para a veiculação ou espaço de ação ou omissão de condutas ilícitas, para ameaças, roubo de dados e informações, danificação do computador ou da rede, verificamos a realização de um ataque cibernético ou ciberataque[1] ("Ciberataque"), colocando diversos elementos do Estado em cheque.

Nas palavras de Clarke e Knake, o Ciberataque *"é a penetração não autorizada, em nome ou em apoio de um governo de outra nação computador ou rede, ou qualquer outra atividade que afeta um sistema de computador, no qual o objetivo é adicionar, alterar ou falsificar dados ou causar o rompimento ou danos a um computador, ou dispositivo de rede, ou os objetos de controles do sistema de computador".*

[1] CLARKE, Richard A.; KNAKER, Robert K. Cyberwar: The Next Threat to National Security and What to Do About It. Tradução: Ramos, Maria Sharlyany MarqueNew York: Ed. Harper Collins. 2010, p.228.

2.1. Soberania dos Estados

A soberania dos Estados, vista por muitos doutrinadores como um dos elementos essenciais do Estado Moderno se configura, no plano fático, como um elemento volitivo ou anímico e de manifestação ou expressão de ordem e de poder por parte dos Estados.[2]

Em uma linha de evolução histórica, tal elemento se mostrou presente desde os tempos das comunidades primitivas, exercido de forma difusa, por meio de anciãos e líderes religiosos que determinavam os rumos de suas sociedades por meio de suas determinações, e conseguiam manter o controle de suas comunidades primitivas, pois essas acreditavam que seus mandamentos decorriam da vontade divina. Tal teoria é expressão da doutrina da natureza divina dos governantes.[3]

Em um segundo momento, verifica-se as soberanias personalistas, exercidas por meio da concentração do poder do Estado nas mãos de um único líder, como bem se verifica as monarquias absolutistas, os Impérios, e os Reis.[4]

O terceiro momento, que se estreita ao vivenciado atualmente, é uma soberania institucional, em que o exercício do poder é balanceado por meio da distribuição de finalidades e competências a órgãos e instituições que detém atividades e limites específicos de atuação do poder. A legitimidade desse poder se dá justamente pelo prévio estabelecimento em Cartas ou Constituições que estabeleçam as competências e a repartição de funções entre as instituições.[5]

[2] DALLARI, Dalmo de Abreu. Elementos de Teoria Geral do Estado. São Paulo: Editora Saraiva. 2 ed. 1997, capítulo II
[3] BONAVIDES. Paulo. Ciência Política. 10 ed. São Paulo: Editora Malheiros, 2000. Capítulo 9
[4] STRECK, Lenio Luiz; MORAIS, Jose Luis Bolzan de. Ciência Política & Teoria do Estado. 8 ed. São Paulo: Editora Livraria do Advogado, 2013. p. 161
[5] MIRANDA. Jorge. Teoria do Estado e da Constituição. Rio de Janeiro: Fonrense, 2005.p, 214

Jean Bodin foi inédito ao estudar, de forma sistemática, o conceito de soberania, dedicando um capítulo inteiro do seu livro "Os Seis Livros da República"[6], livro primeiro, para conceituar tal tema. O autor, ao tempo da escrita de tal livro, encontrava-se imerso na França do século XVI, que se apresentava como um ambiente hostil, marcado pela supremacia do poder político e por disputas religiosas entre católicos e protestantes.

Nessa atmosfera, Jean Bodin inaugurou a ideia de que, em meio ao caos, descobre-se a necessidade do exercício da soberania, a qual deveria ser realizada por meio da concentração do poder nas mãos do monarca, dando poder à própria monarquia.[7]

A mesma posição compartilha Baker, ao mencionar:

> *"foi o medo da anarquia, consequência necessária, segundo ele, da doutrina de resistência legítima dos 'monarcômanos', que incitou Bodin a sustentar que, para preservar a ordem social, cumpria que se exercesse uma vontade soberana suprema. Para ser soberana, afirmava ele, essa vontade deve necessariamente ser unitária. E para ser unitária impõe-se necessariamente que seja perpétua, indivisível (portanto, inalienável) e absoluta; em consequência independente do julgamento ou do comando de outrem."*[8]

Bodin acreditava que a soberania se tratava de um poder perpétuo absoluto, que, ainda que amparado pela lei, cabia ao próprio monarca, a criação e exclusão das mesmas. Logo, verificava-se o exercício de um poder superior, independente, ilimitado e incondicional por parte do monarca.

---

[6] BODIN, Jean. Os seis livros da república. Trad. José Carlos Orsi Morel (v. 1)/ José Ignacio Coelho Mendes Neto (vs. 2-6). Rev. José Ignacio Coelho Mendes Neto. São Paulo: Ícone, 2011. (6 v.)

[7] SKINNER, Quentin. The Foundations of Modern Political Thought, vol.2: The Age of Reformation, 19th printing, Cambridge: Cambridge University Press, 2013, p.284.

[8] BAKER, K. M. "Soberania". In: FURET, F. Dicionário crítico da Revolução Francesa. Rio de Janeiro: Nova Fronteira, 1989, p.882.

Nas palavras de Jean Bodin: "*É preciso que o soberano possa dar a lei aos súditos e anular ou revogar as leis inúteis para fazer outras; o que não pode ser feito por aquele que está submetido às leis ou por aquele que está sob o comando de outrem."* (República I, 8, p. 191).[9]

Para o inglês Thomas Hobbes, que também viveu em um período de guerras e disputas políticas e religiosas avençadas entre a Coroa e o Parlamento, a denominada Revolução Gloriosa, o homem em seu estado natural e inerte vive pautado em desconfianças, criatividade e insegurança, trazendo sempre à sociedade pensamentos de disputa.[10]

Foi nessa perspectiva que Hobbes criou a premissa de que o "homem é o lobo do próprio homem" e que somente o "Estado" constituído por um poder e normas seria capaz de evitar tal estado natural do homem.[11]

Para o pensador inglês, a constituição desse Estado se dava por meio de um pacto social, firmado por um contrato que submetia os indivíduos, quisessem eles ou não, às normas e poderes do Estado Soberano*, "considerando e reconhecendo cada um como Autor de todos os atos daquele que representa sua pessoa praticar, em tudo o que se refere à Paz e à Segurança Comuns."*[12]

Vivenciado o mesmo contexto político, histórico e religioso de Hobbes, surge o pensador John Locke que, diferentemente de Hobbes, entende que o estado natural do homem é de busca pela paz e liberdade, por meio da resistência civil. Assim, e justamente por conta desse estado de espírito do homem, que se permite aos indivíduos o discernimento entre poder legítimo dos soberanos e poder repressivo, imperativo e desumano.[13]

[9] CHEVALLI ER, Jean Jacques. As grandes obras políticas: de Maquiavel a nossos dias. Tradução de André Praça de Souza Teles .8 ed. Rio de Janeiro: AGIR,2001, p.124 .
[10] HOBBES, Thomas. Leviatão, ou, Matéria, forma e poder de um Estado eclesiástico e civil.5 ed. São Paulo: Martil Claret, 2011, p.95.
[11] HOBBES, 2011, p.106 - 107.
[12] HOBBES, 2011, p.126 – 127.
[13] AZAMBUJA, Darcy. Teoria Geral do Estado. 2 ed. São Paulo: Editora Globo, 2008, p.59.

Tal tese é reforçada, sobretudo, na obra *Dois tratados sobre o Governo* (1690) quando o autor identifica que o Estado soberano é legítimo a partir do momento que, por meio do discernimento, os indivíduos consentem com o pacto social, admitindo a existência do Estado Soberano. Dessa forma, o poder soberano é decorrência da vontade da maioria, não podendo, portanto, ser contrário às leis e normas que também foram instituídas por vontade da maioria, que, se não for cumprida, instigará a natureza de resistência do homem, razão pela qual, legitima-se o poder soberano, na visão de Locke.[14]

Anos mais adiante, influenciado pelo Iluminismo, surge o pensador Jacques Rousseau que começava a identificar no contratualismo de Hobbes e Locke um grupo de indivíduos que, pautados pelo contrato social, aceitavam o poder que lhes era imposto, todavia, não detinham qualquer mecanismo de voz e representação.

> *"[...] os deputados do povo não são, nem podem ser, representantes seus; são comissários dele, e nada podem concluir decisivamente. É nula, nem é lei, aquela que o povo em peso não ratifica. Julga-se livre o povo inglês, e muito se engana, que o é só durando a eleição dos membros do parlamento, finda a qual, hei-lo na escravidão, hei-lo nada; e como ele emprega os breves momentos de sua liberdade, merece bem que o perca."*[15]

Foi então, no século XVIII, com os anseios da Revolução Francesa que Rousseau lança sua ideia de que, de fato, há um Contrato Social entre os indivíduos e o poder soberano, porém, esse último não pode ser legitimado somente pela imposição ou consentimento, mas também por meio do funcionamento e participação da máquina política. De modo que o soberano seja funcionário do povo como forma de legítima soberania.[16]

[14] LOCKE, John. Dois tratados sobre o Governo. Tradução de Julio Fischer. São Paulo: Martins Fontes, 2005, II, c.19.
[15] ROUSSEAU. Do contrato social. São Paulo: Martin Claret, 2003, p. 91-92
[16] ROUSSEAU, 2003, p.92

Tal acepção, apesar de devidas adaptações às circunstâncias de cada Estado é a que parece minimante a se estreitar ao conceito de soberania vivenciada pelas democracias atuais, como descreve o Professor Paulo Bonavides:

> *"povo e Nação formam uma só entidade, compreendida organicamente como ser novo, distinto e abstratamente personificado, dotado de vontade própria, superior às vontades individuais que o compõem. A Nação, assim constituída, se apresenta nessa doutrina como um corpo político vivo, real, atuante, que detém a soberania e a exerce através de seus representantes".*[17]

O que se depreende é que, apesar das diferenciações e justificativas que cada autor confere ao Estado Soberano, às instituições ou à pessoa do soberano em si, todos buscam demonstrar que o fortalecimento do poder, por meio da centralização do mesmo, é a forma de se conferir soberania aos Estados.

Nesse sentido, a soberania do Estado moderno apresenta características marcantes, quais sejam a unicidade, indivisibilidade, a inalienabilidade e a imprescritiblidade. Una, pois não se admite em um mesmo Estado a convivência de mais de um poder superior, devendo este ser único e expressão do somatório das vontades individuais.

A decorrência dessa característica é a forma indivisível que deve ser exercida essa soberania, pois, da mesma forma que o povo, democraticamente, confere a uma unidade o poder soberano, esse deve ser exercido perante a totalidade dos fatos que estão sob o seu poder, não podendo dividir ou escolher quais fatos estarão submetidos ou não àquela soberania.

Cabe ressaltar que a existência de repartição de poderes, de divisão de funções e competências não ataca as características aqui mencionadas, uma vez que a unidade e indivisibilidade não está restrita a uma pessoa física ou jurídica, expressamente dita.

[17] BONAVIDES, Paulo. Ciência Política. 10.ed. São Paulo: Malheiros, 2002, p.131-132.

Inalienável em virtude do poder soberano não poder ser objeto de alienação, o que não impede, todavia, que seja delegado como repartição das funções e, finalmente, imprescritível pois não se delimita tempo ao exercício da soberania que, via de regra, tem caráter vitalício[18]

2.2. Guerra Física vs Guerra Cibernética

De acordo com o Estatuto de Roma, ratificado no Brasil por meio do Decreto nº 4.388, de 25 de setembro de 2002[19], em linhas gerais, crimes de guerra são aqueles crimes que: (i) violam os direitos estipulados na Convenção de Genebra, a qual, em termos gerais, dispõe sobre os Direitos Humanitários Internacionais; e (ii) violam leis e costumes aplicáveis a um conflito bélico, em âmbito internacional ou não.

Apesar do legislador ter reservado o artigo 8º[20] do referido decreto para arrolar os crimes de guerra e as especificidades de cada um dos possíveis crimes, o que se verifica em comum a eles é que todos dependem de uma ação humana, com a produção de um resultado no plano fático para ser configurado como um crime de guerra.

Isso porque o tipo penal atribuído aos crimes de guerra tem como núcleo central ações/omissões humanas que prescindem de um resultado fático. Cita-se como exemplo do referido Decreto:

[18] AZAMBUJA, Darcy. Teoria Geral do Estado. 2 ed. São Paulo: Editora Globo, 2008, p.66.

19 BRASIL. Decreto nº. 4.388 de 25 de setembro de 2002.Promulga o Estatuto de Roma do Tribunal Penal Internacional. Brasília,DF, set 2002

[20] BRASIL. Decreto nº. 4.388 de 25 de setembro de 2002. *"Art. 8º. 1. O Tribunal terá competência para julgar os crimes de guerra, em particular quando cometidos como parte integrante de um plano ou de uma política ou como parte de uma prática em larga escala desse tipo de crimes.2. Para os efeitos do presente Estatuto, entende-se por "crimes de guerra"(...)"*

> *"2. Para os efeitos do presente Estatuto, entende-se por "crimes de guerra":*
>
> *a) As violações graves às Convenções de Genebra, de 12 de Agosto de 1949, a saber, qualquer um dos seguintes atos, dirigidos contra pessoas ou bens protegidos nos termos da Convenção de Genebra que for pertinente:*
>
> *i) Homicídio doloso;*
>
> *(...)*
>
> *b) Outras violações graves das leis e costumes aplicáveis em conflitos armados internacionais no âmbito do direito internacional, a saber, qualquer um dos seguintes atos:*
>
> *i) Dirigir intencionalmente ataques à população civil em geral ou civis que não participem diretamente nas hostilidades;*
>
> *(...)*
>
> *c) Em caso de conflito armado que não seja de índole internacional, as violações graves do artigo 3o comum às quatro Convenções de Genebra, de 12 de Agosto de 1949, a saber, qualquer um dos atos que a seguir se indicam, cometidos contra pessoas que não participem diretamente nas hostilidades, incluindo os membros das forças armadas que tenham deposto armas e os que tenham ficado impedidos de continuar a combater devido a doença, lesões, prisão ou qualquer outro motivo*
>
> *(...)*
>
> *iii) A tomada de reféns;"*

Nos três exemplos elencados acima (i) homicídio; (ii) dirigir intencionalmente ataques; e (iii) tomada de reféns torna-se mais claro que os crimes de guerra, em geral, produzem efeitos no campo físico, decorrente de uma conduta humana. Uma vez que não é possível configurar o homicídio sem (i) a ação humana de matar e; cumulativamente (ii) o resultado fático e provado da morte de um indivíduo.

Em mesma linha é o entendimento do exemplo de dirigir intencionalmente ataques à população civil. Prescinde-se (i) a ação humana; (ii) intencional de atacar, não importando, nesse caso, o meio e a forma que ocorre o ataque e; ainda (iii) o resultado fático de prova da ocorrência do ataque às populações civis.

Nesse exemplo, é viável, atualmente, com o desenvolvimento da tecnologia, pensar em mutação no conceito do termo ataque de modo que, ainda que careça da ação humana, este pode ser praticado no ambiente virtual.

Como último exemplo do Decreto que conceitua os crimes de guerra, temos a tomada de reféns. Tal ação, assim como as ilustradas acima, dependem de uma (i) ação humana; e (ii) a submissão do indivíduo ao sequestrado, configurando-se como refém.

Atualmente, ainda que não se possa denominar propriamente como refém, diversos indivíduos, entes governamentais e empresas privadas são constrangidas a cumprir exigências, por meio de Ciberataques, para que um resultado prático não seja produzido, como por exemplo, no caso da Netflix que diversos países foram constrangidos a pagar alta quantias para não terem seus conteúdos de mídia digitais disseminados.

Diante dessa conjuntura, nota-se que os crimes de guerra que, por conceituação do Decreto nº. 4.388 de 25 de setembro de 2002, ainda que dependam de uma (i) ação ou omissão humana; e (ii) uma produção de um resultado fático, não estão restritos às ações realizadas no âmbito "real", podendo ser realizadas no "âmbito" virtual, sem descaracterizar o conceito.

Nesse sentido, o monopólio do uso da força detido, antigamente, aos Estados[21], que expressavam tal monopólio pelo poder bélico, hoje pode ser detido por todo e qualquer indivíduo. Isso porque, as ações virtuais não carecem de um mandamento Estatal ou governamental para serem realizadas, podendo ter sua origem por indivíduos de menor porte de seus computadores ou meios tecnológicos caseiros. Essa possibilidade traz como resultado um aumento nos ataques virtuais, tendo em vista, a menor complexidade e o baixo valor dos mesmos.

[21] WEBER, Max. Economia e sociedade. Brasília: Editora UNB, 1991. Volume I, capítulo I e III, p. 3-35; 139-162. Volume II, p. 517-580.

Como consequência, os Estados, os inimigos, os combatentes que antes tinham identidade definida e pública, converte-se em figuras, na maioria das vezes, anônimas capazes de realizar ataques.

Por fim, em decorrência do próprio conceito *weberiano* de Estado pautado no monopólio do uso da força, a guerra que antes representava para os Estados e indivíduos como um meio de prover segurança, capaz de gerar efeitos práticos e físicos, como mortes, ferimentos, conquistas de territórios, alterações de fronteiras geográficas e etc, hoje pode ser analisada como uma ameaça à soberania e a própria existência de Estado.[22] De modo que a guerra não é vista, nos dias atuais, como a única forma do Estado prover segurança.

Para Freund, o entendimento quanto ao conceito de Estado era também pautado em uma visão norteada pelo uso da força ou de uma entidade dotada de tal poder, intitulada em nome do Estado. Assim diz o autor quanto ao caráter do monopólio da força:

> "(...) *a esse caráter específico do Estado, acrescentam-se outros traços: de um lado, comporta uma racionalização do Direito com as consequências que são a especialização dos poderes legislativo e judiciário, bem como a instituição de uma polícia encarregada de proteger a segurança dos indivíduos e de assegurar a ordem pública; de outro lado, apoia-se em uma administração racional baseada em regulamentos explícitos que lhe permitem intervir nos domínios os mais diversos, desde a educação até a saúde, a economia e mesmo a cultura. Enfim, dispõe de uma força militar, por assim dizer, permanente."*[23]

Em resumo, com a transição dos conceitos mencionados neste capítulo, a guerra mudou de plano de existência, de modo que o conflito bélico e físico passou a ser travado em um ambiente virtual. Nesse sentido, as características de guerra foram se transformando de maneira

[22] WEBER, Max. "A política como vocação". in M. Weber, Ciência e política: duas vocações. Tradução de Jean Melville. São Paulo: Martin Claret, 2003, p.10
[23] FREUND, Julien. Sociologia de Max Weber. Trad. Luís Cláudio de Castro e Costa. 2. ed. Rio de Janeiro: Forense, 1975, p. 159.

que, hoje, a guerra não é travada e declarada por opção e por uso, necessariamente, da força dos Estados. Nota-se que diversos são os possíveis atores de uma guerra, inclusive sem o amparo essencial seja de um Estado, um governo, ou um poderio bélico e/ou militar.

Ademais, com a possibilidade de diversos agentes aliados ao uso da tecnologia no contexto de guerra, o anonimato se tornou uma premissa da guerra cibernética, sem que seja, nos dias de hoje, motivo de honra demonstrar de onde ou quem produziu determinado resultado criminoso.

Isso porque, as distâncias físicas das ações já não mais importam, pois, a tecnologia e o ciberespaço ultrapassam as fronteiras físicas das guerras travadas também no plano físico. Diante disso, apesar do resultado atingir escalas globais, as ações têm menor custo e complexidade, de modo que indivíduos e atores de menor porte têm a capacidade de produzir resultados que antes eram de capacidade exclusivamente dos Estados.

Finalmente, em contraponto aos combates físicos, os combates virtuais não representam uma forma de manter a segurança de um Estado e de seus indivíduos, mas sim, uma fraqueza nas formas de proteção dos dados, da rede, das informações e dos meios tecnológicos disponíveis às vítimas dos Ciberataques.

QUADRO I – Características do combate físico e virtual

FÍSICO	VIRTUAL
Monopólio do uso da força pelo Estado	Diversidade de atores, inclusive de menor porte, com a possibilidade de anonimato
A movimentação de recursos para um combate é de grandes portes e alto valor	Ataque quase sem custos
Ataque restrito à territorialidade pretendida	A distância física e o local de ataque não são delimitados

Função de prover segurança aos indivíduos e forma de mostrar poder	A insegurança e soberania dos Estados é colocada em cheque com a verificação de Ciberataques

Fonte: Elaboração a partir do autor NYE.

Para Joseph Nye[24], as barreiras do mundo virtual são pequenas, de forma que atores não-estatais ou ainda, Estados de pequeno porte poderiam exercer funções relevantes e com baixos custos. Em contraposição aos domínios do espaço aéreo ou do mar que, diante do alto custo e da complexidade demandada, está, na maioria das vezes, restrita à atuação de atores Estatais.

Para Arquilla e Ronfeldt[25], ciberguerra pode ser definido como:

> *"[...] conduzir e preparar para conduzir, operações militares de acordo com os princípios da informação [...] Esta forma de guerra pode envolver diversas tecnologias – nomeadamente C3I; recolha de informação, posicionamento e identificação de amigos ou inimigos (IFF); e sistemas de armas "inteligentes" – para dar apenas alguns exemplos. Pode também envolver interferência electrónica, falseamento, sobrecarga e intrusão nos circuitos de informação e comunicação de um adversário. [...] Poderá também implicar o desenvolvimento de novas doutrinas sobre o tipo de forças necessárias, onde e como deslocá-las, e saber o quê e como atacar no lado do inimigo. Como e onde posicionar determinados tipos de computadores e sensores relacionados, redes, bases de dados, etc., pode-se tornar tão importante como a questão que costumava ser efetuada sobre deslocação de bombardeiros e as suas funções de suporte. A ciberguerra pode também ter implicações para a integração dos aspectos políticos e psicológicos com os aspectos militares de fazer a guerra.*"[26]

[24] NYE, Joseph S. Cyber Power. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Disponível em: < http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf >

[25] ARQUILLA, John; RONFELDT, David. Cyberwar is Coming! (Ed.). In: Athena's Camp: preparing for conflict in the information age. Santa Monica CA: Rand Corp, 1997. p. 23. (Reedição do artigo originalmente publicado na Comparative Strategy, v. 12, n. 2, 1993)

[26] ARQUILLA, John; RONFELDT, David, Cyberwar is Coming! (Ed.). In: Athena's Camp: preparing for conflict in the information age. Santa Monica CA: Rand Corp, 1997, p.30-31. (Reedição do artigo originalmente publicado na Comparative Strategy, v. 12, n. 2, 1993)

2.3. *Jus ad bellum e Jus in bello*

Tendo em vista a recente comparação da guerra cinética com a guerra cibernética, entende-se que os princípios aplicáveis àquela deverão ser observados também nesta. Dessa forma, as regras e princípios gerais que regem o Direito Internacional e os Estados quando diante de um combate devem ser aplicados também nos contextos de combates virtuais, com suas devidas adaptações.

Via de regra, o Direito Internacional em Combates Armados leva em conta dois tipos de direito relacionados ao uso da força, são eles o *jus ad bellum* e o *jus in bello.* O entendimento relacionado a este último, segundo Rezek é que o *jus in bello* diz respeito ao direito de guerra, isto é, são normas, costumes e convenções que existiam ao tempo em que os Estados viam a guerra como uma opção lícita e quase que única viável para a resolução de conflitos.

Nesse conceito de *jus in bello*, não era realizada, primordialmente, uma ponderação do cabimento da guerra para a resolução do conflito, de modo que a guerra por vingança, para restituição de bens indevidos ou para afagar sofrimentos de povos era vista como uma opção.[27]

Já no contexto do *jus ad bellum*, há uma ponderação do que seria uma guerra justa para que haja um controle dos combates e guerras admitidas pelos Estados. Tal provisão parece minimizar os combates que são fruto de uma herança sangrenta da história da humanidade.

A Carta da ONU estabelece, como regra, em seu art.2º:

[27] REZEK, José Francisco. Direito internacional público: curso elementar – 11 ed. ver e atual – São Paulo: Saraiva, 2008, capítulo II, parágrafo 260

> *"Art.2º .Todos os membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os propósitos das ações Unidas" (NAÇÕES UNIDAS, 1945).*[28]

Logo, depreende-se uma proibição quanto ao uso da força e à ameaça por um Estado. Entretanto, levando-se em conta o *jus ad bellum*, em algumas circunstâncias excepcionais entende-se legítimo o uso da ameaça e do uso da força. Inclusive, na própria Carta da ONU faz essa ressalva, insculpida nos art.39 e 51. Os mencionados dispositivos garantem o uso legítimo da força desde que, por meio da autorização do Conselho de Segurança e diante de um ataque armado que requer ao Estado a legítima defesa. Observa-se:

> *"Art.51. Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um membro das ações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos [sic] membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais (NAÇÕES UNIDAS, 1945)."*

Ainda que, ao tempo da elaboração de tal norma inexistia a realidade de Ciberataques por parte dos Estados, ao transladar, analogicamente o entendimento dessa orientação normativa para o campo da prática internacional sobre o assunto, ainda que obscuro o limite interpretativo, deve-se manter válido, como norma geral norteadora do próprio direito internacional o *jus ad bellum*.

Nessa perspectiva, para Shackelford, a interpretação do termo "força" trazido pela Carta da ONU, ainda que gere debates, não está restrito e limitado somente na sua adequação ao contexto cinético de guerra, relacionado especificamente a armamentos militares e bélicos. O

[28] SÃO FRANCISCO. Estatuto da Corte Internacional de Justiça. Carta das Nações Unidas, 1945

que importa, para o autor são os efeitos que se busca alcançar pelo termo e não os meios utilizados.[29]

Assim, entende-se que a limitação do uso da força estabelecida pela ONU objetiva minimizar os efeitos devastadores de uma guerra, independente da modalidade e forma que ela seja travada, bélica, militar, nuclear, biológica ou cibernética.

Para Hubert Thierry, o legado sangrento marcado pelas duas grandes guerras do século XX, conduziu a humanidade pela busca de justiça, de paz, de segurança, em contraponto ao longo período vivenciado de violação dos direitos fundamentais e dos crimes contra a humanidade, da degradação do meio ambiente em decorrência da ação humana. Foi assim que a própria concepção do direito foi se transformando, de forma a se adequar à nova realidade e demanda de uma sociedade que buscava se afastar do legado e do fardo do século passado.[30]

Nas palavras do autor:

> *"O direito não é somente conjunto de técnicas, mas também e sobretudo, conjunto de princípios e de normas. Sob esse aspecto o direito internacional também consideravelmente progrediu no curso de nosso século", e isso se exprime na medida em que "antes da primeira guerra mundial o direito internacional era sobretudo o direito das relações entre as potências europeias, que levavam em seu rastro, para o melhor e para o pior, o resto do mundo. Mas esse direito que chamam de "clássico", era muito rudimentar. O recurso à guerra não era proibido, e constituía, antes, o exercício do "jus ad bellum", concebido como atributo da soberania. O direito internacional regulamentava, bem ou mal, a divisão colonial e regia as formas e as modalidades da colonização. As obras publicadas após a segunda guerra mundial refletem as normas a esse respeito, que permaneciam em vigor, nessa época anterior à formação do direito da descolonização. As relações entre os estados e os seus*

[29] SHACKELFORD, Scott J. From nuclear war to net war: analogizing cyber attacks in international law. Berkeley Journal of International Law. v. 27, n. 1, p. 192-251, 2009. Disponível em: <http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7>.

[30] CASELLA, Paulo Borba; ACCIOLY, Hidelbrando; SILVA, G.E do Nascimento E. Manual de direito internacional público. — 20. ed. — São Paulo : Saraiva, 2012, cap 8.1.

> *próprios nacionais fundamentavam-se essencialmente na competência nacional, o que excluía a proteção internacional dos direitos do homem".*[31]

2.4. O ciberespaço

William Ford Gibson, escritor californiano, é considerado o pai do termo "ciberespaço" ao escrever, em 1984, o livro "Neuromancer"[32]. Tal obra conta a história de um *hacker* que encontra no ciberespaço um ambiente suscetível de praticar crimes que não poderiam ser praticados com a mesma facilidade (e anonimato) que no mundo físico e real. Apesar de se tratar de um romance de ficção científica, o livro pode ser representado como um marco histórico, por introduzir à sociedade diversos conceitos e ideias inovadoras para a época.

Apesar de o termo, inicialmente, ter sido relacionado ao mundo fictício das novelas, atualmente, ele vem ganhando maior notoriedade, relacionado, na maioria das vezes, com temas ligados à tecnologia, crimes de internet e inovações virtuais.

Ainda que não exista um conceito fechado, é possível notar o ciberespaço como um ambiente em que computadores ou meios tecnológicos são utilizados, por meio da conexão de internet entre eles, seja por uma rede pública, privada ou doméstica. Nesse mesmo sentido Lucia Leão vê o ciberespaço:

> *"Camaleônico, elástico, ubíquo e irreversível, o ciberespaço não se reduz a definições rápidas. Partindo de um olhar tríplice, percebemos que o ciberespaço engloba: as redes de computadores interligadas no planeta (incluindo seus documentos, programas e dados); as pessoas, grupos e instituições que participam dessa interconectividade e, finalmente, o espaço (virtual, social, informacional,*

[31] THIERRY, Humber. L'évolution du droit international: cours général de droit international public. Paris: RCADI, 1990, t. 222, p. 24-26.

[32] GIBSON, W. Neuromancer. Trad. de Alex Antunes (baseada na tradução da 1ª ed. de Maya Sangawa e Silvio Alexandre). 3. ed. São Paulo: Aleph, 2003

cultural e comunitário) que emerge das inter-relações homens-documentos-máquinas"[33]

Diferente do meio físico, em que as ações e omissões ocorrem em momentos diferentes e até mesmo distantes do resultado, o ciberespaço é uma zona, não visível necessariamente, em que que uma ação e/ou omissão seja simultânea à produção de um resultado. Ademais, no ciberespaço a própria ação ou omissão não depende, essencialmente, da presença física do homem.

Pierre Lévy faz referência ao ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Para o professor, o ciberespaço permitiu que os espaços antes delimitados territorialmente por cidades, estados e países sejam conectados, de modo a "desterritorializar" a realidade. Desse modo, verifica-se um redirecionamento do tempo e do espaço real, para a dimensão virtual.[34]

Nessa perspectiva, o ciberespaço passou a ter importante papel não só na relação entre o homem e os seus meios tecnológicos, como computadores, celular, pagers, e rádios, mas principalmente na relação entre os próprios homens.

É presumível que, por meio da tecnologia e da criação desse novo espaço, a interação social deixou de se limitar ao espaço físico, ganhando horizontes mais largos, ao passo que as fronteiras foram sendo quebradas pela existência de dois mundos paralelos: a realidade real, limitada aos espaços físicos e a realidade virtual, que não comporta uma delimitação territorial. De modo que, criou-se mais um espaço em que o risco é suscetível para as sociedades humanas, decorrente da situação paradoxal de sucesso desse novo meio.

[33] LEÃO, Lucia. Derivas: cartografias do ciberespaço. São Paulo. Annablume, 2004, p.9
[34] LÉVY, Pierre, Qu'est-ce que le virtuel?.Paris, Éditions La Découverte, coll. Sciences et Sociéte, 1995, p.157

Em outras palavras, verificado um novo ambiente de êxito, em que há uma facilitação das atividades que antes dependiam do mundo físico, viu-se uma brecha para a o uso desse ambiente como um meio de instrumentos destrutivos da própria sociedade.[35]

[35] FERNANDES, José Pedro Teixeira. Da utopia da sociedade em rede à realidade da sociedade de risco. Análise Social, 207, xlviii (2.º), pp. 260-286. Lisboa, Portugal. 2013.

3. CIBERATAQUE COMO FENÔMENO JURÍDICO

Os ataques cibernéticos verificados nos últimos tempos passaram a ser utilizados não somente como um teste da capacidade tecnológica de indivíduos comuns, mas principalmente como uma forma de deter poderio político, financeiro e econômico. A tecnologia, que antes era o fim em si mesmo, passou a ser instrumento para alcance de objetivos finais de conflitos reais.

Na medida que algum acontecimento exterior ou não ao homem apresenta-se como importante para a concretização da ordem e/ou justiça, ele se torna capaz, então, de produzir impactos nos direitos dos indivíduos, Estados, ou entes personalizados ou não. Esse impacto, que carece de uma tutela por parte do Direito – nesta acepção como área de conhecimento – transforma tal acontecimento como um fenômeno jurídico.

Desse modo, como mencionado acima, os Ciberataques tem se mostrado como mais uma modalidade de infração aos direitos do Estado moderno, sendo verificado, muitas vezes por meio de prática de ações ilícitas ou delituosas, gerando efeitos práticos no mundo real.

Logo, além da necessidade de criação de métodos de defesa em face de ataques cibernéticos, o Ciberataque visto como fenômeno jurídico traz ao século atual a necessidade de criação, também, de legislações, tratados e questões diplomáticas que, em conjunto com os meios tecnológicos, auxiliem na neutralização dos impactos jurídicos que um Ciberataque pode causar.

3.1. Definições jurídicas e elementos essenciais

Com o desenvolvimento da Internet e da tecnologia, o uso da rede mundial de computadores também foi sofrendo mutações em razão das motivações e resultados pretendidos, adequados a diferentes circunstâncias econômicas, políticas e sociais.

Quando antes a Internet era muito rudimentar e limitada, seu uso era extremamente restrito a funções e demandas simples, como por exemplo, o envio de documentos digitais. Com o desenvolvimento tecnológico e a adequação de necessidades das sociedades, a Internet passou

a ser utilizada como meio de comunicação, método de ensino, auxílio na área de saúde e até substituição de mão de obra humana.

Atualmente, diante do seu sucesso nos mais variados âmbitos aplicáveis, seu uso vem sofrendo diárias mutações. Foi nesse contexto que os próprios Ciberataques também sofreram variações, podendo ser classificados de formas distintas, de acordo com o resultado pretendido pelo ataque virtual.

Para Keniche Guimarães Matsuyama e João Ademar de Andrade Lima[36], a primeira e mais primitiva forma de Ciberatataque, são os ataques de natureza comum, também denominados puros, isso porque a finalidade dos ataques se resume em atacar e invadir o sistema computacional alheio e seus componentes. Isto é, a investida do agente tem como escopo afetar o equipamento físico, o sistema informático e as informações dos bancos de dados. Nessa espécie temos, por exemplo, a invasão de servidores e sites.

Já no ataque cibernético misto, o agente se utiliza do sistema computacional alheio, sem necessariamente causar danos físicos a esse sistema, visando bem jurídico distinto. Nessa hipótese, a tecnologia é meio primordial para a concretização do ataque, como é o caso, por exemplo, de ataques de navegação de serviço.

Por fim, estão os ataques comuns, que recebem essa denominação, pois a rede mundial de computadores é o ambiente do qual se vale um agente para realizar conduta ilícita que já esteja tipificada no Código Penal, como, por exemplo a fraude de contas bancárias.

A crescente exponencial desse último tipo de ataque, os ataques comuns, se verifica, pois, atividades do dia-a-dia que antes se efetivavam por meio do papel, como por exemplo, transações bancárias, documentos de identificação, passagens eletrônicas, ingressos, etc, atualmente, vem sendo substituídas por meios tecnológicos como códigos de barras, QR code, aplicativos, validações digitais e etc.

[36] MATSUYAMA, K. G.; LIMA, J. A. A. Crimes cibernéticos: atipicidade dos delitos. Disponível em: <http://www.cedipe.com.br/3cbpj/docs/artigos_pdf/11_crimes_ciberneticos_atipicidade_dos_delitos.pdf.>

Nesse âmbito de substituição dos documentos de papel, o Ciberataque se demonstra como um fenômeno de grande impacto na vida social dos indivíduos como, também, no meio jurídico. Visto que, evidências e meios de proteção e coerção que se davam no plano físico não são mais suficientes e, ainda, a falta de legislações que determinem procedimentos padrões de uso das tecnologias e de efetivação da segurança no meio virtual, tornam a Internet um ambiente hostil para a prática de ataques.

4. COMBATE AOS CIBERATAQUES

As potencialidades do ciberespaço, por possibilitarem uma conexão imediata e direta de pessoas e informações, têm cooperado para uma grande migração e desenvolvimento de sistemas que atendem as populações que antes se encontravam vinculados a burocracias físicas para o ciberespaço, de modo a otimizar e melhorar a qualidade de vida dos indivíduos.

Essa migração e consequente dependência do novo espaço virtual gera um dever de cuidado do mesmo, uma vez que nele estão inseridos sistemas não só do setor privado como de atendimento às necessidades básicas da população, como abastecimento de água, energia, saúde, transporte, financeiro e telecomunicações.[37]

Nesse aspecto, se por um lado o ciberespaço representa um ambiente de facilitação e melhoria na vida dos indivíduos, se mostra também um ambiente que chama a atenção para a prática de atos de grande comoção e mobilização, representados nesse estudo como os Ciberataques.

Diante do relevante impacto no mundo real gerado por um Ciberataque, surge a necessidade de combate aos mesmos. Entretanto, a dificuldade desse combate surge quando os Ciberataques, por característica, não estão limitados a um território e, ainda, não tem um agente definido, sendo praticados, via de regra, por agentes anônimos.

Esses elementos fazem questionar a soberania, a competência e a jurisdição dos Estados nos limites de seus esforços em combater o Ciberataque.[38] Diante desse dilema, tornou-se importante a desconstrução de fronteiras de modo que o Estado soberano fosse redimensionado em face dos novos desafios da modernidade , surgindo a necessidade de busca pela solução por meio da cooperação entre os Estados.[39]

[37] MOREIRA, João Manuel Dias. O impacto do ciberespaço como nova dimensão nos conflitos. Lisboa: Boletim Ensino. Investigação nº 13, 2012, p. 27-50

[38] GOLDSMITH, Jack. The Internet and the Legitimacy of Remote Cross-Border Searches. Chicago public law and legal theory working paper no. 16 – p.4. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732

[39] MIRANDA, Napoleão. Globalização, Soberania Nacional e Direito Internacional. Brasília: R. CEJ, n.27, Out-Dez/.2004.

4.1. Formas de cooperação jurídica internacional entre os Estados

O direito, ciência social que, como o próprio o nome faz referência, deve atender às demandas sociais, adequando-se aos diversos contextos globais em que é aplicado. Inclusive, não sendo possível dissociar o Direito da função social que é seu dever desempenhar.[40]

Desse modo, em um mundo globalizado em que as relações sociais, econômicas e interpessoais ocorrem cada vez mais de forma dinâmica, verificando-se, inclusive, o contato e o relacionamento de indivíduos e entes situados em localidades, territórios e países distintos, surgiu a necessidade, da criação de formas que garantissem o intercâmbio internacional para o cumprimento de providências extraterritoriais no âmbito judicial. Foi, então, dentro do direito internacional privado o berço da criação de mecanismos que facilitassem e auxiliassem o contato entre os Estados por meio da cooperação jurídica.[41]

Diante da globalização e da vasta troca de informações a nível global, as demandas judiciais vêm, proporcionalmente, alcançando e demandando a apuração de fatos e informações em escala global. Assim, há um exponencial crescimento na necessidade de intercâmbio internacional para o cumprimento de medidas administrativas e processuais em âmbito extraterritorial, observando-se o aumento da cooperação jurídica entre os Estados e entes administrativos, por meio de diversas modalidades de cooperação, assistência ou auxílio.

Esse câmbio de diligências entre Estados, que antes era realizada por livre arbítrio e reverência para com o outro Estado sofreu remodelamentos, em face das vultuosas demandas de diligências.

Para Rodrigo Otávio[42], a cooperação entre os Estados vai além da posição de cortesia e condescendência entre os Estados, pois essas dependem de uma decisão arbitrária do Estado que pode ser revogada ou não realizada a qualquer tempo, por livre e espontânea vontade do próprio estado. Para o referido autor, a cooperação jurídica internacional gera um dever

[40] NADER, Paulo. Introdução ao estudo do direito. 36 ed. Rio de Janeiro: Forense, 2014, cap. 2
[41] ARAÚJO, Nadia de. Direito Internacional Privado: Teoria e Prática Brasileira. 6 ed. Porto Alegre: Revolução eBook, 2016, capítulo III
[42] OTAVIO, Rodrigo, Direito Internacional Privado, Parte Geral, Rio de Janeiro, Ed. Freitas Bastos, 1942, p. 115.

obrigacional entre os Estados que, ainda que não seja baseado em um dispositivo necessariamente vinculante, gera uma obrigação moral entre as nações, transformando a mera faculdade em uma imposição ao Estado como forma de integração política no contexto global e no bom convívio e relacionamento internacional.

Da mesma visão compartilham Nádia Araújo e Lauro Gama Jr.[43], pela percepção que, por meio da cooperação jurídica internacional, há a conversão do compromisso moral (*comitas gentium)*, tornando-se uma obrigação jurídica.

Ademais, além da questão das grandes demandas de cunho transnacional e da necessidade-utilidade de bons relacionamentos no plano da comunidade internacional percebe-se um crescente no reforço de direitos reconhecidos no plano internacional que demandam proteção, também, a nível global. Como exemplo, os direitos humanos, as diretrizes de usos e costumes do comércio internacional, os direitos do cidadão.[44]

Tais direitos se mostram tão relevantes para os dias atuais que a cortesia internacional não é mais suficiente para garantir a efetividade dos mesmos, vislumbrando-se, portanto, uma relação direta e vinculante entre os Estados, de forma extraterritorial, para que as garantias sejam respeitadas.

A grande questão que envolve os meios de cooperação jurídica internacional é que, justamente, por envolverem nações e Estados diversos, evidencia-se, de igual forma, diversidades de circunstância fáticas, jurídicas e legislativas entre as partes envolvidas nos esforços de cooperação e auxílio mútuo.

Neste cenário, há uma responsabilidade dos Estados em perseguir uma codificação internacional, com intuito de uniformizar, no plano global, possíveis soluções administrativas e judiciais, por meio de tratados e convenções internacionais e, ao mesmo tempo, satisfazer as

[43] ARAÚJO, Nadia de; GAMA JUNIOR, Lauro. Sentenças estrangeiras e cartas rogatórias: novas perspectivas da cooperação internacional. Disponível na Internet: <http://www.mundojuridico.adv.br/sis_artigos/artigos.asp?codigo=51>.

[44] ABADE, Denise Neves. Direitos fundamentais na cooperação jurídica internacional: extradição, assistência jurídica, execução de sentença estrangeira e transferência de presos. São Paulo: Saraiva, 2013.

perspectivas e os direitos das partes que estão submetidas ao poder do Estado, que em última instância, são os indivíduos partes do processo que deu ensejo à necessidade da cooperação.[45]

Nesses esforços em criar de meios de cooperação jurídica internacional para combater os Ciberataques, os princípios de jurisdição devem ser analisados. O principal deles é a soberania territorial, que para Joseph Story, é a posse de cada nação de exclusiva soberania e jurisdição dentro de seu próprio território. A consequência desse princípio é a vedação das nações em interferir, por leis nacionais, diretamente na propriedade, sociedade, direito ou indivíduos de outro Estado.[46]

Vale ressaltara a palavra chave do conceito acima, qual seja, "diretamente". Logo, admite-se a regulação extraterritorial de pessoas e propriedades, por meio de leis nacionais, desde que seja realizada de forma indireta, ou seja, desde que por meio do auxílio ou consentimento do Estado que se busca a cooperação.[47]

Por conseguinte, a mudança que vem se verificando ao longo dos tempos não está necessariamente na forma que um Estado auxilia o outro, mas sim o escopo da influência extraterritorial. Ao longo da história, o escopo que permite interferência de um Estado sobre outro vem se expandindo de modo a se adequar à lógica fática vivenciada, de modo que, atualmente, a necessidade tecnológica e virtual é uma demanda relevante para que os Estados se auxiliem mutuamente.

Uma manifestação concreta da mudança nesse conceito pode ser vista em 2013 quando, um juiz norte americano instaurou a busca e apreensão de contas de e-mail hospedadas pela Microsoft no banco de dados do programa Outlook, na Irlanda. A decisão foi contestada sob fundamento de violação às normas de direito internacional, uma vez que a diligência buscava,

[45] GOLDSMITH, Jack. The Internet and the Legitimacy of Remote Cross-Border Searches. Chicago public law and legal theory working paper no. 16 – p.4. Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732

[46] STORY, Joseph. Comentaries on the Conflict of Laws Foreign and Domestic, In Regard to Contracts, Rights and Remedies, And Especially in Regard to Marriages, Divorces, Wills, Successions and Judgments. 2 ed. Little, Brown: 1841, parágrafo 18 e 20

[47] GOLDSMITH, Jack. The Internet and the Legitimacy of Remote Cross-Border Searches. Chicago public law and legal theory working paper no. 16 – p.6. Disponível em <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732>

em última instância, a realização de um ato unilateral dos Estados Unidos, sem a utilização de meios de cooperação internacional para obtenção de provas no exterior.[48]

Frente a esse caso e a necessidade do uso da cooperação jurídica internacional para o atendimento de demandas tecnológicas e virtuais, tornou-se necessário o lançamento de duas perspectivas para a concretização dos interesses dos Estados: por um lado, o Estado deve manter sua soberania e satisfazer o interesse dos seus particulares; por outro, ele deve ser visto como parte em um contexto global, devendo respeitar os princípios e tratados da comunidade internacional.

Logo não é praticável que um Estado admita e forneça meios de diligências a outro Estado em desacordo com a soberania exercida perante seus indivíduos, somente para o bom relacionamento no exterior. À contrário senso, tampouco é concebível que um Estado abra mão de princípios e tratados que é parte internacionalmente para dar total e irrestrito cumprimento de solicitações de seus indivíduos. Para Mueller, a ponderação e o equilíbrio dessas duas perspectivas não ameaçam a soberania, mas pelo contrário, reafirmam a soberania dos Estados em uma era cibernética.[49]

4.2. Princípios básicos

A cooperação jurídica internacional voltada para efetivação de medidas processuais para apuração de crimes ou ilícitos penais ganhou tamanha representatividade que um dos princípios fundamentais que rege esse câmbio de diligências é a aplicação da norma mais favorável à cooperação (*favor comissionis* ou *pro solicitudine)*.

Esse princípio decorre da procura de harmonia nas relações internacionais de forma que o atendimento ao ato solicitado é uma regra internacional e deve ser acatado de melhor maneira não ao Estado, tampouco ao requerente ou ao requerido do pedido, mas sim, ao próprio pedido.

---

[48] MADRUGA, Antenor, FELDENS, Luciano. Dados eletrônicos e cooperação internacional: limites jurisdicionais. Temas de cooperação internacional / Secretaria de Cooperação Internacional. Brasília:MPF,2015, p.47

[49] MUELLER, M.L. The Global Politics of Internet Governance. Cambridge: The MIT Press. Massachusetts Institute of Technology, p.1-271, 2010. Disponível em: <http://pages.uoregon.edu/koopman/courses_readings/phil123-net/intro/mueller_networksand-states.pdf>.

Em consequência, a impossibilidade de cumprimento deve ser fundamentada e justificada, de maneira a não infringir direitos fundamentais envolvidos na própria solicitação.

Em contraponto ao princípio do *favor comissionis*, Ada Pellegrini Grinover destaca que, ainda que, de certa forma seja antagônico à necessidade de intensificação da cooperação jurídica na luta contra o crime, deve estar sob conhecimento cada vez mais intrínseco dos Estados o respeito aos direitos fundamentais do indivíduo que deve estar como plano primordial de correspondência da matéria, devendo ser vistos como limites à cooperação internacional. Como por exemplo, princípios processuais penais básicos como a ampla defesa, a duração razoável do processo, o direito das vítimas, presos e acusados e o contraditório devem ser vistos em primeiro plano, não podendo ser olvidados em favor da melhor produção da diligência.[50]

Frente ao desafio do dever de prestar informação na seara da cooperação em medidas processuais penais e o respeito aos direitos fundamentais, cada vez em maior escala são ratificados tratados multilaterais com o intuito de facilitar e dar celeridade às solicitações de diligências entre os Estados, positivando princípios e direitos básicos que devem ser respeitados mutuamente ente os Estados.[51]

4.3. Marco Civil da Internet (Lei nº 12.965/2014)

No Brasil, foi somente em 2014 quando se criou uma legislação que alcançasse a realidade social e virtual que o processo de globalização trouxe ao país. A utilização cada vez em maior escala do ciberespaço trouxe a necessidade de estabelecer princípios, garantias e deveres para o uso da Internet no Brasil de forma a prevenir e evitar a utilização indevida dessa ferramenta.

Além da conceituação, como forma de prevenção do mau uso, a Lei 12.965/2014[52] dispõe, em seu artigo 11, de forma implícita a possibilidade de coleta de dados na Internet por meio de Estados estrangeiros. Veja-se:

[50] GRINOVER. Ada Pellegrini. Processo penal transnacional: linhas evolutivas e garantias processuais. Revista Brasileira de Ciências Criminais, n.9: São Paulo, 1995, p.40-83

[51] WEBBER, Patrícia Maria Núñez. Cooperação internacional penal: conceitos básicos. Temas de Cooperação Internacional / Secretaria de Cooperação Internacional – Brasília: MPF, 2015, p.34

[52] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.Brasília, 23 de abril de 2014.

> *"Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.*
>
> *§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.*
>
> *§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. [...]"*

O dispositivo, ao estabelecer que a realização de "pelo menos um desses atos" se realizados em território nacional deve respeitar a legislação brasileira, entende-se que, admitiu-se, implicitamente, a hipótese de que algum ou todos os atos de coleta possam ocorrer fora do território nacional.

Esse dispositivo, ainda que timidamente, demonstra os esforços ainda a passos curtos do legislador brasileiro em inserir-se no contexto do ciberespaço e, ainda, de ressaltar a importância de tratamento legislativo a esta seara, principalmente, em vista das possibilidades, à época da promulgação da referida lei, de necessidades de cooperação jurídica internacional para apuração de diligências em face de crimes praticados no âmbito virtual.[53]

4.4. A Convenção de Budapeste

Na Europa, a preocupação com o estabelecimento de conceitos, princípios e garantias que envolvessem a Internet e o ciberespaço se deu no início dos anos 2000, quando em 2001

[53] MADRUGA, Antenor, FELDENS, Luciano. Dados eletrônicos e cooperação internacional: limites jurisdicionais. Temas de cooperação internacional / Secretaria de Cooperação Internacional. Brasília:MPF,2015, p.61

foi criada a Convenção de Budapeste, também denominada "Convenção sobre o Cibercrime", em vigor desde 2004.

A referida legislação, logo em seu preâmbulo, tipifica diversos crimes dentro do direito penal material deixando clara a prioridade por *"uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional"*, bem como reconhece a *"necessidade de um cooperação entre Estado e a indústria privada"*.

O que chama atenção da Convenção de Budapeste é que diversas problemáticas vivenciadas pelos Estados e elencadas neste estudo são resolvidas no próprio texto da lei. Primeiramente, a dificuldade de conceituação de cibercrimes, aqui denominados Ciberataques, que é definido pela Convenção como infrações contra sistemas e dados informáticos (Capítulo II, Título 1), infrações relacionadas com computadores (Capítulo II, Título 2), infrações relacionadas com o conteúdo, pornografia infantil (Capítulo II, Título 3), infrações relacionadas com a violação de direitos autorais (Capítulo II, Título 4). Todos dentro do Direito Penal Material.

Em segundo lugar, a dificuldade de se estabelecer a competência e jurisdição dos Estados em razão do anonimato e não territorialidade dos Ciberataques é resolvida pela Convenção ao estabelecer, em seu art.22, que as Partes poderão adotar, a seu critério, qual será a jurisdição mais apropriada para o procedimento legal.

Para Castells, a *"internacionalização das atividades criminosas faz com que o crime organizado (...) estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização, em vez de lutar entre si"*[54]. Na conceituação do autor, a Convenção parece buscar esse papel.

Cabe ressaltar que, ainda que a Convenção tenha caráter transnacional, sendo aplicável a diversos países da Europa, ela expressamente resguarda as especificações das legislações nacionais, ao dispor em seu art.15 que:

[54] CASTELLS, Manuel. Fim do Milênio. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3)., p.205

> *"Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade."*

Tal ressalva é de suma importância pois expressamente garante e ainda reforça as soberanias nacionais que muitas vezes se sentem ameaçadas ao aderir à tratados que estabeleçam princípios, direitos e deveres relacionados ao ciberespaço e ao Ciberataque. Somado a isso, a Convenção, ainda que estabeleça procedimentos de cooperação jurídica entre os Estados, estimula a produção legislativa dos Estados no intuito de combater os ataques virtuais. Veja-se o art. 16:

> *"Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração."*

Atualmente, a Convenção conta com 72 países signatários, dentre eles países que, inclusive, não são parte da Europa, são eles: Argentina, Austrália, Cabo Verde, Canadá, Chile, Colômbia, Costa Rica, República Dominicana, Gana, Israel, Japão, Ilhas Mauricio, México, Marrocos, Nigéria, Panamá, Paraguai, Peru, Filipinas, Senegal, África do Sul, Sri Lanka, Tonga, Tunísia e Estados Unidos.

Nota-se o êxito da Convenção em razão da quantidade de signatários e, principalmente, em virtude da sua inovação em lançar mão de conceitos de extrema importância para realidade fática que careciam de um entendimento minimamente padronizado e globalizado para que

houvesse um entendimento conjunto entre os Estados em realizar um combate, também conjunto, aos Ciberataques.

Ademais, a Convenção é de extrema importância prática pois ainda que estabeleça alguns procedimentos padrões para a efetividade da cooperação jurídica internacional, ela dispõe de orientações e diretrizes que podem auxiliar os próprios Estados a se auxiliarem mutuamente por meios não necessariamente jurídicos, mas também tecnológicos, técnicos, políticos, legislativos e diplomáticos.

Nesta seara, diversas outras opções de cooperação foram tomando forma internacionalmente, criando sistemas e procedimentos que, em última instância, trouxessem ao mundo fático o desenho positivado na Convenção de Budapeste.

4.5. Política de Ciberdefesa da OTAN

Diante dos riscos relacionados à segurança de seus países membros, por conta de Ciberataques, e ciente de que a cooperação entre os Estados é medida efetiva para a neutralização de ataques virtuais, a OTAN impulsionou uma Política de Ciberdefesa que, não se ateve somente à criação de conceitos jurídicos e principiológios, mas principalmente à criação de medidas técnicas de efetivação dos mandamentos e diretrizes contidas nas leis esparsas sobre Internet, ciberespaço e, principalmente, à Convenção de Budapeste.

Por meio dessa política, determinou-se a centralização de redes de computadores, de modo a facilitar a comunicação de sistemas de defesa para a criação de um relatório com diagnóstico de vulnerabilidades. Por meio dessa política, são fornecidos equipamentos de análise de vulnerabilidade, bem como de assistência jurídica por meio da investigação ou atualização normativa, que auxiliam na identificação de vulnerabilidades.[55]

Se por um lado as ações de combate aos Ciberataques realizadas individualmente pelos Estados membros da OTAN se tornam limitadas em face da conexão dos sistemas de defesa, por outro lado há um caminho concreto e efetivo realizada em conjunto, dada a, ainda,

[55] Instituto Nacional da Defesa Nacional. Estratégia da Informação e Segurança no Ciberespaço nº 12. Lisboa: Cadernos do IDN, 2013, p.59-63

fragilidade técnica e legislativa verificada na estrutura interna dos Estados para encarar o problema.

4.6. União Europeia (EU)

Após o sucesso da Convenção de Budapeste e a grande adesão de países da união europeia, surgiu a necessidade da criação de métodos não somente jurídicos, mas principalmente técnicos no controle às ameaças cibernéticas no âmbito da União Européia.

Diante disso, iniciou-se, em 2008, a Estratégia de Segurança Europeia, posteriormente atualizada em 2013, que se trata de um plano de ação comum aos Estados da União Europeia, focalizando as principais ameaças na área dos crimes cibernéticos e propondo ações de melhoria, prevenção e combate, todos realizados por meio da cooperação entre os Estados.[56]

Por meio desses documentos o ciberespaço é tratado como ambiente essencial para a promoção dos direitos humanos. Assim, A União Europeia vem adotando uma política de ciberseguraça baseada no modelo da OTAN, criando um vínculo entre a ciberdefesa e as operações de segurança, denominada Política Comum de Segurança e Defesa (*Common Security and Defense Policy)*[57]

Portanto, a unificação de legislação, por meio da Convenção de Budapeste, e de medidas práticas de mapeamento e segurança vem colocando a União Europeia em posição avançada para o compartilhamento de estratégias de defesa, bem como de ente capaz de promover a atenção que o ciberespaço requer.

[56] RSP 2013/2606. Resolução do Parlamento Europeu sobre a estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido. 2013. Disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//PT

[57] PIRES, H.F. Estados Nacionais, Soberania e Regulação da Internet. Barcelona: Revista Eletrônica de Geografia y Ciencias Sociales, v.XVI, n.418, Nov/2012. Disponível em: <http://www.ub.edu/geocrit/coloquio2012/actas/12-H-Pires.pdf>.

4.7. ONU

Em razão dos danos proporcionados pelos Ciberataques, a proteção às tecnologias de informação e comunicação foi incluída como pauta na Aassembleia Geral das Nações Unidas. Tal inclusão deu ensejo a resoluções que pretendem[58]:

(i) Proteger a liberdade do fluxo de informação da utilização criminosa da internet – A/RE/53/61;
(ii)Propor a cooperação legislativa e política – A/RES/56/121;
(iii) Criação de uma cultura global de cibersegurança – A/RES/57/239;
(iv) Desenvolver a integração da infraestrutura crítica – A/RES64/211; e
(v) Promover a coordenação em cibersegurança a nível mundial;

A preocupação da ONU com a cibersegurança deixa clara a escassez dos recursos que detêm os Estados para promover, individualmente, ações de proteção dos seus próprios ciberespaço. Desse modo, organizações com melhor infraestrutura e mais recursos, como a ONU são necessárias para auxiliar a proteção dos Estados.[59]

4.8. O Caso Brasileiro de proteção ao espaço cibernético e das infraestruturas críticas

O Brasil, reconhecido mundialmente como uma potência econômica em expansão, vem adotando progressos científicos e tecnológicos em suas estruturas de forma a otimizar as atividades desempenhadas na política, economia, saúde, educação e justiça.

Tal crescimento e relevância do Brasil no âmbito internacional, vem chamando atenção de *hackers* para um ambiente suscetível para a prática de condutas ilícitas por meio dos novos sistemas tecnológicos. Inclusive, durante a 7ª Cupúla Latino-americana de Analistas de

[58] KOHONA,P.T.B. The United NationsTreatyon The Internet. The American Journal of International Law, Vol.92,No 1,Jan.2009, p.140-148. Disponível em:<http://www.jstore.org/stable/2998074>. Acesso em: 31/05/2016. Além de ter participação ativa nas políticas de cooperação em cibersegurança, a Organização das Nações Unidas (ONU) também presidiu a celebração de vários tratados sobre a internet, ao ponto de criar uma verdadeira compilação digital, com a finalidade de facilitar a difusão do conhecimento de suas premissas, facilitando sua aplicabilidade.

[59] PIRES, H.F. Estados Nacionais, Soberania e Regulação da Internet. Barcelona: Revista Eletrônica de Geografia y Ciencias Sociales, v.XVI, n.418, Nov/2012. Disponível em: <http://www.ub.edu/geocrit/coloquio2012/actas/12-H-Pires.pdf>

Segurança da Kaspersky Lab foi anunciado que o Brasil lidera a posição onde ocorrem maiores incidentes de roubo de dados na América Latina[60].

Essa posição, que de um lado se mostra extremamente benéfica para a reputação do país mundialmente, também faz surgir uma preocupação na busca de estratégias de defesa e segurança dos sistemas tecnológicos que estão propiciando tal crescimento. Assim, foram criadas diversas equipes de resposta e tratamento de incidentes em redes.

Por exemplo, o denominado Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal[61], o Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa[62], o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil[63], além de diversos outros grupos de segurança espalhados pelo território nacional, com intuito de coibir ou neutralizar Ciberataques praticados em face de empresas privadas ou órgãos governamentais.

Isso decorre do fato que diversas atividades, que são essenciais para as atividades do Estado, que antes eram realizadas por meios físicos, foram migradas, nos últimos anos, para sistemas informacionais, conectados por meio da rede mundial de computadores. Essa migração, passou a englobar as atividades do Estado brasileiro como infraestruturas críticas, as quais são instalações, serviços, bens e sistemas que, se forem atacados, descontinuados ou cessados causam grande comoção e impacto social, podendo colocar em risco à segurança do Estado e da Sociedade.[64]

A importância de tais infraestruturas na vida cotidiana dos indivíduos que dela dependem e, inclusive, no funcionamento do Estado requer um cuidado relevante diante do cenário de Ciberataques nota-se em crescimento. Portanto, foi criada uma Política Nacional de

---

[60] Dados disponíveis em <https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-digital-kidnappings-in-latin-america>

[61] Vide: <http://www.ctir.gov.br/>.

[62] .Vide: <http://www.rnp.br/cais/>.

[63] Vide: <http://www.cert.br/>

[64] Portaria nº 45 de 8 de setembro de 2009, do GSI/PR: Artigo 2º. Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas. § 2º São Infraestruturas Críticas as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade. Disponível em: < http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009 >

Segurança da Informação[65] que estabelece pressupostos, objetivos e diretrizes que devem ser seguidos em âmbito nacional pelos diversos órgãos e entidades da Administração Pública como forma de evitar e combater de forma padronizada os ataques ou ameaças cibernéticas.

No que tange o relacionamento externo do Brasil na missão de combate aos Ciberataques no cenário mundial, foi elaborado, em 2010, pelo Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República – DSICGSI o Livro Verde sobre Segurança Cibernética no Brasil[66] ("Livro Verde").

A referida norma objetiva, além de reforçar diretrizes e normas orientadoras estabelecidas em portarias esparsas, estabelecer uma proposta de articulação de acordos e tratados internacionais, com o objetivo de fortificar e formentar a segurança cibernética no país, bem como aumentar as capacidades de defesa e dissuasão, por meio da cooperação internacional.

Veja-se que um capítulo do Livro Verde foi reservado nesse intuito:

> *"COOPERAÇÃO INTERNACIONAL*
>
> *PROMOVER a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento da estratégia nacional de segurança cibernética;*
> *INSTITUCIONALIZAR no país a autoridade nacional de segurança, no curto prazo, com vistas a oficializar e sistematizar o processo de credenciamento de órgãos, entidades, empresas, e pessoas para intercâmbio de informações classificadas, entre governos;*
> *PROMOVER E ARTICULAR acordos de cooperação técnica de segurança cibernética, no curto, médio e longo prazo;*

[65] BRASIL.Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000

[66] BRASIL. Livro verde: segurança cibernética no Brasil/Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações: organização Claudia Canongia e Raphael Mandarino Junior – Brasília: GSCIPR/SE/DSIC, 2010 p.63

> *PROMOVER visão alinhada e consensada entre os atores-chave atuantes na segurança cibernética, no curto, médio e longo prazo, visando a definição de posicionamento estratégico do país, no tema, em fóruns, comitês e colegiados internacionais;*
> *ESTABELECER programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, no curto, médio e longo prazo;*
> *ARTICULAR acordos internacionais de modo a potencializar a segurança cibernética do País, sua capacidade de defesa e dissuasão, além do aumento e atualização das suas competências essenciais."*

Desse modo, observa-se os esforços do Brasil em adotar medidas semelhantes às adotadas pela OTAN, União Europeia e ONU, especialmente, no que se refere ao estímulo de articulação internacional para a promoção da segurança cibernética internacional. Tal estímulo não se dá somente no que tange os acordos e tratados internacionais, como, ainda, a adoção de medidas técnicas eficazes ao combate direto às agressões virtuais, expressado, especialmente, nos seguintes trechos do capítulo de cooperação jurídica internacional do Livro Verde:

> "*ESTABELECER programas de cooperação específicos (...) com outros Governos e a comunidade internacional, no curto, médio e longo prazo;*
> *ARTICULAR acordos internacionais de modo a potencializar a segurança cibernética do País, sua capacidade de defesa e dissuasão, além do aumento e atualização das suas competências essenciais."*

4.9. Tratamento pelo Código de Processo Civil de 2015

A cooperação jurídica internacional praticada no ordenamento jurídico brasileiro até o ano de 2015 era usualmente amparada por leis, regulamentos, regimentos, tratados esparsos e presentes da Resolução nº 9/05 do STJ[67]. Com o incremento do processo de globalização e um aumento no fluxo de relações comerciais, interpessoais, institucionais e de serviços estabelecidos constantemente, tais como contratos internacionais, divórcios entre pessoas de nacionalidades de diferentes e processos de natureza cível e criminal que transcendem fronteiras, o legislador brasileiro reservou um capítulo exclusivo do Código de Processo Civil

[67] BRASIL Superior Tribunal de Justica. Resolução nº 9 de 4 de maio de 2005. Dispõe, em caráter transitório, sobre competência acrescida ao Superior Tribunal de Justiça pela Emenda Constitucional nº 45/2004.

de 2015 – CPC para tratar do tema da cooperação internacional que, cada vez mais, vem se tornando uma prática constante no judiciário.

Em seu art. 26, o CPC apresenta regras gerais de Cooperação Internacional, deixando clara a importância dos Tratados Internacionais para a efetivação das diligências extraterritoriais. Inclusive, o art. 13 do CPC demonstra expressamente que o tratado, convenção ou acordo internacional em matéria civil que o Brasil tenha legalmente aprovado e ratificado no ordenamento jurídico pátrio deva ser respeitado em detrimento da lei nacional. Nessa perspectiva, a aplicação de um tratado internacional não é uma questão de conveniência e oportunidade por parte do Brasil, mas sim uma obrigação perante à Comunidade Internacional.[68]

> *"Art. 13. A jurisdição civil será regida pelas normas processuais brasileiras, ressalvadas as disposições específicas previstas em tratados, convenções ou acordos internacionais de que o Brasil seja parte."*

Inclusive, havendo tratado, convenção ou acordo firmado entre Partes que necessitam da troca de diligências entre si, admitiu-se pela nova redação do CPC o auxílio direito entre as Partes, realizados por meio de autoridades centrais, dispensando a vinculação de órgãos jurisdicionais. Somado a isso, as diligências não estão restritas ao âmbito judicial, podendo se estender para providências judiciais e extrajudiciais. Veja-se o art. 30 do CPC:

> *"Art. 30. Além dos casos previstos em tratados de que o Brasil faz parte, o auxílio direto terá os seguintes objetos:*
> *I - obtenção e prestação de informações sobre o ordenamento jurídico e sobre processos administrativos ou jurisdicionais findos ou em curso;*
> *II - colheita de provas, salvo se a medida for adotada em processo, em curso no estrangeiro, de competência exclusiva de autoridade judiciária brasileira;*
> *III - qualquer outra medida judicial ou extrajudicial não proibida pela lei brasileira."*

Essa modalidade de cooperação entre países permite uma celeridade e efetividade de medidas que se mostram urgentes ou essenciais para o andamento de decisões judiciais e/ou

[68] ARAÚJO, Nádia. Inclusão de regras sobre cooperação jurídica internacional no novo CPC: O novo sistema harmônico brasileiro. Revista Cooperação em pauta. n. 2, março/2015.

administrativas. Diante da essencialidade do auxílio direito, o CPC criou um rol não taxativo de formas que os Estados podem se auxiliar mutuamente, evidenciado pelo inciso "*qualquer outra medida judicial ou extrajudicial não proibida pela lei brasileira"*.

Na lição de Ricardo Perlingeiro Mendes da Silva[69]:

> *"(...)a preferência pela expressão 'cooperação jurídica internacional' decorre da idéia de que a efetividade da jurisdição, nacional ou estrangeira, pode depender do intercâmbio não apenas entre órgãos judiciais, mas também entre órgãos judiciais e administrativos, de estados distintos."*

Portanto, havendo dispositivo normativo que permita o uso do auxílio direto, dispensa-se a utilização de meios mais demorados e que envolvam, necessariamente, o judiciário para a efetivação de providências judiciárias e/ou administrativas.

Nesse sentido, o STJ já se manifestou ao determinar que, havendo tratado ou convenção entre os Estados para o cumprimento de diligências por meio de auxílio direito, não há razão de ser para o envio de cartas rogatórias, uma vez que esse procedimento seria contrário à própria lógica do auxílio direto e da cooperação internacional, qual seja a eficiência e celeridade das diligências. Veja-se:

> *"HABEAS CORPUS . EVASÃO DE DIVISAS (ARTIGO 22 DA LEI 7.492/1986). QUEBRA DE SIGILO DE CONTA BANCÁRIA NO EXTERIOR. ACORDO DE ASSISTÊNCIA JURÍDICA EM MATÉRIA PENAL CELEBRADO ENTRE OS GOVERNOS BRASILEIRO E DOS ESTADOS UNIDOS DA AMÉRICA - MLAT. PROMULGAÇÃO PELO DECRETO 3.810/2001). ALEGADA INAPLICABILIDADE A CRIMES CONSIDERADOS LEVES. INEXISTÊNCIA DE RESTRIÇÃO NO MENCIONADO INSTRUMENTO JURÍDICO. ILEGALIDADE NÃO CARACTERIZADA.*
>
> *1. Da leitura do item 4 do artigo 1º do Acordo de Assistência Jurídica em Matéria Penal - MLAT, percebe-se que os Governos do Brasil e dos Estados Unidos da América reconhecem a especial importância em combater os graves crimes ali listados, sem, contudo, excluir a apuração de outros ilícitos, já que não há limitação ao alcance da assistência mútua a ser prestada, de modo que a simples afirmação de*

[69] SILVA, Ricardo Perlingeiro Mendes da Silva. O direito internacional contemporâneo – estudos em homenagem ao professor Jacob Dolinger. Rio de Janeiro: Renovar, 2006, p. 798.

que o delito de evasão de divisas não estaria previsto no mencionado dispositivo legal não é suficiente para afastar a sua incidência na hipótese, uma vez que, como visto, o rol dele constante não é taxativo, mas meramente exemplificativo. 2. Aliás, já na introdução do Acordo tem-se que o Brasil e os Estados Unidos pretendem "facilitar a execução das tarefas das autoridades responsáveis pelo cumprimento da lei de ambos os países, na investigação, inquérito, ação penal e prevenção do crime por meio de cooperação e assistência judiciária mútua em matéria penal", ou seja, por meio dele os Governos almejam o auxílio no combate aos delitos em geral, e não com relação a apenas algumas e determinadas infrações penais. 3. Por sua vez, no item 1 do artigo 3º do Acordo estão enumeradas as restrições à assistência, dentre as quais não se encontram crimes considerados leves, notadamente o de evasão de dividas. ALEGADA IMPRESTABILIDADE DO MLAT POR VIOLAÇÃO DO PRINCÍPIO DA IGUALDADE. APONTADA UTILIZAÇÃO DO ACORDO APENAS PARA O ATENDIMENTO DE PEDIDOS FORMULADOS NO INTERESSE DA ACUSAÇÃO. POSSIBILIDADE DE A DEFESA PLEITEAR A PRODUÇÃO DA PROVA AO JUÍZO, QUE A SOLICITARÁ AO ESTADO REQUERIDO. INCONSTITUCIONALIDADE NÃO EVIDENCIADA[70]"

Ainda em mesmo sentido decidiu o Ministro Sebastião Reis Júnior, ao julgar o Recurso em Habeas Corpus interposto em face de decisão que negou seguimento ao Habeas Corpus impetrado para controlar a ação do Tribunal Regional Federal da 4ª Região que julgou que as provas obtidas pelo Brasil nos Estados Unidos foram lícitas, em razão de um tratado internacional que permitia a cooperação entre os Estados Parte.

A recorrente fundamenta a ilicitude das provas em razão de que diligência já havia sido prestada pelo Estado requerido. A sexta turma do STJ, todavia, denegou o recurso sob a ótica que, uma vez existindo tratado válido entre as partes, o auxílio direto poderá ser prestado, sem limitação, enquanto perdurar a validade e eficácia do tratado que regula a cooperação e relação dos Estados parte.

"DIREITO PROCESSUAL PENAL. LICITUDE DA PROVA. COMPARTILHAMENTO DE DADOS E INFORMAÇÕES OBTIDOS VIA MLAT (MUTUAL LEGAL ASSISTANCE TREATY). OPERAÇÃO OURO VERDE. 1. O tratado MLAT firmado entre Brasil e Estados Unidos da América não contempla a especialidade como regra; pelo contrário, estabelece que a restrição ao uso da prova

[70] HABEAS CORPUS Nº 147.375 – RJ. Rel. Ministro Jorge Mussi – 5ª Turma STJ. Data de julgamento: 22 de novembro de 2001

> *é que constituirá exceção, dependendo de manifestação expressa e cristalina, o que não ocorreu. 2. Há nos autos diversas e expressas manifestações da autoridade norte-americana facultando o uso irrestrito da prova fornecida ao Estado brasileiro, inclusive mediante consulta com referência inequívoca à operação Cabo Verde.*
> *(...)*
> *Além disso, como explica Vladimir Aras, os órgãos do Ministério Público e do Judiciário do Estado requerente podem reportar-se diretamente, por ofício, por telefone ou por email, à autoridade central de seu próprio país, assim como à autoridade central do Estado requerido, para obter informações sobre o andamento das solicitações (O sistema de cooperação penal Brasil/Estados Unidos. Cooperação jurídica internacional em matéria penal/organizadores José Paulo Baltazar Junior, Luciano Flores de Lima. Porto Alegre: Verbo Jurídico, 2010, pág. 362).*
> *(...)*
> *O pedido de cooperação direta, não obstante deva preencher certos requisitos caracteriza-se pela informalidade e não necessita da intervenção do Poder Judiciário (a propósito, a Resolução n. 9/STJ). Neste feito, a controvérsia diz respeito à necessidade e à inobservância, no caso, da regra de especialidade para o uso de prova obtida por meio do Acordo de Assistência Judiciária em Matéria Penal firmado entre o Governo da República Federativa do Brasil e o dos Estados Unidos da América – MLAT, o qual prevê mecanismos bastante flexíveis de intercâmbio de informações."*[71]

No mesmo entendimento filia-se, ainda que indiretamente, o STF por meio da Súmula Vinculante nº 10[72] que afirma que a não aplicabilidade ou o afastamento de incidência de lei ou ato normativo do Poder Público viola cláusula de reserva de plenário. Logo, havendo lei, tratado ou convenção válidos que determine procedimentos de auxílio direto, sua não aplicabilidade corresponde à violação direto ao próprio ordenamento jurídico.

> *"SÚMULA VINCULANTE Nº 10. Viola a cláusula de reserva de plenário (CF, artigo 97) a decisão de órgão fracionário de tribunal que, embora não declare expressamente a inconstitucionalidade de lei ou ato normativo do Poder Público, afasta sua incidência, no todo ou em parte."*

Ainda nessa esteira, o STF entende a vinculação e independência dos tratados internacionais e do auxílio direto estabelecido por meio deles, ao afirmar que, nessas hipóteses,

[71] RECURSO EM HABEAS CORPUS Nº 42.825 – RS. Rel. Ministro Sebastião Reis Júnior – 6ª Turma STJ. Data de Julgamento: 1 de setembro de 2015
[72] BRASIL. Supremo Tribunal Federal – Súmula Vinculante nº 10.

não há que se falar de *exequatur* a ser conferido pelo STJ para conferir validade e eficácias às providências solicitadas entre os Estados partes. Veja-se:

> *"AGRAVO REGIMENTAL EM FACE DE DECISÃO MONOCRÁTICA DE RELATOR NO STF. PEDIDO DE COOPERAÇÃO JURÍDICA INTERNACIONAL. AUXÍLIO DIRETO. PLEITO DO MINISTÉRIO PÚBLICO PORTUGUÊS. TRATADO DE AUXÍLIO MÚTUO EM MATÉRIA PENAL. DECRETO 1.320/94. OITIVA DE PRESO. CUSTÓDIA PARA FINS DE EXTRADIÇÃO SUBMETIDA AO STF. COMPETÊNCIA. CARTA ROGATÓRIA E EXEQUATUR NO STJ. DESNECESSIDADE. AGRAVO PROVIDO. 1. O pedido de cooperação jurídica internacional, na modalidade de auxílio direto, possui natureza distinta da carta rogatória. Nos moldes do disposto nos arts. 28, 33, caput, e 40, todos do Código de Processo Civil, caberá auxílio direto quando a medida não decorrer diretamente de decisão de autoridade jurisdicional estrangeira, enquanto necessitará de carta rogatória quando for o caso de cumprir decisão jurisdicional estrangeira. 2. Formulado pedido de assistência direta pelo Ministério Público português ao Parquet brasileiro, com base em tratado internacional de mútua cooperação em matéria penal, firmado entre Brasil e Portugal Decreto 1.320/1994, o cumprimento em território pátrio depende de mero juízo de delibação, sendo desnecessária a atuação homologatória em exequatur pelo Superior Tribunal de Justiça. 3. Encontrando-se o preso sob a custódia do Supremo Tribunal Federal, para fins de extradição, a esta Corte deve ser dirigida a comunicação de que o custodiado será ouvido em razão de pedido de cooperação formulado pela autoridade central portuguesa e encaminhado ao Ministério Público brasileiro. 4. Agravo regimental provido".*[73]

[73] Petição nº 5946 no Agravo Regimental – DF – Rel. Ministro Edson Fachin – 1ª Turma do STF . Data de julgamento: 16 de agosto de 2016

CONCLUSÃO

O presente trabalho é fruto da perplexidade em face da incessante inovação tecnológica que vem ocorrendo nos últimos anos. Todos os dias é possível descobrir uma nova tecnologia, um novo dispositivo, uma nova rede social e um novo meio de se estabelecer conexões pelo mundo.

Se por um lado tais conexões permitem a dinamicidade e a evolução da vida humana na terra, quando se utiliza a tecnologia a favor, seja no âmbito da saúde, da economia, da política, da justiça e do conhecimento, é possível, por outro lado, verificar a utilização das redes e conexões dinâmicas e constantes para a prática de atos em malefício de indivíduos, sociedades e Estados.

Distâncias encurtadas, informações repassadas em segundos, quebra de barreiras físicas, acesso conteúdos mais vastos em menor tempo, permitiram a fluidez nas relações pessoais e institucionais. Esse ambiente, ao ver de muitos, é o cenário perfeito para valer-se do sucesso e êxito da tecnologia no mundo moderno para deturpar seu uso.

Nesse diapasão, o comportamento humano vem sofrendo mutações e inovações em companhia do desenvolvimento tecnológico. A dependência do homem moderno aos serviços conectados à rede mundial de computadores gera uma vulnerabilidade do próprio conceito de sistemas interligados.

Diante desse contexto, e levando-se em conta a história da humanidade marcada pela constante disputa de poder, de dominação, de exploração da matéria prima disponível até sua escassez, torna-se evidente, após a análise desse estudo que os tempos modernos apresentam uma migração, ainda que não totalmente, da modalidade de guerra e combate físico para a seara do ciberespaço.

Nessa perspectiva, utiliza-se métodos distintos ao longo da história, as motivações dos combates também vão se alterando, o espaço em que os conflitos são travados vão se realocando, mas o homem ainda conserva, em grande parte, o mesmo objetivo, qual seja da dominação e do poder.

Seja pelo território, pelo dinheiro, pelo espaço, pela política, pela religião, pela opção sexual ou racial, mas, ao final, exprime-se pela busca pelo poder.Desse modo, a guerra cibernética vem sendo analisada como mais uma forma de busca pelo poder, em outras palavras, mais uma modalidade de guerra.

Assim, princípios, normas e diretrizes aplicadas ao combate físico vem sendo transportados, com suas devidas adaptações, ao contexto do combate virtual. Uma vez que, em última instância, os efeitos dos Ciberataques surgem no campo físico e visual.

Cabe ressaltar que o presente estudo não tem a pretensão de trazer conceitos fechados, uma vez que, conforme dissertado, e de acordo com diversos autores citados, o tema aqui abordado é de extremamente recente, estando, ainda, sob vivência do homem, razão pela qual não existem conceitos concretos e certeiros quanto aos temas aqui abordados.

Além disso, como se trata de um tema intrinsecamente relacionado à tecnologia, a conceituação se torna ainda mais difícil, visto que todos os dias, a tecnologia se reinventa, podendo alterar conceitos já criados, acrescentando, excluindo, substituindo e criando novos procedimentos, dispositivos e meios virtuais ainda inexistentes no mundo dos fatos.

Passada à análise das conceituações, no que cerne a questão de possíveis soluções para o combate dos Ciberataques, valendo-se do mesmo argumento acima, por se tratar de um fenômeno pouco vivenciado ainda, estando ainda em fase de descobrimento pelo homem moderno, não existem leis, protocolos, tratados ou normas que estabeleçam, concretamente, qual a melhor medida a ser seguida no combate aos ataques cibernéticos.

De maneira oposta, o que vem ocorrendo é um esforço mútuo e contínuo dos Estados em alcançar os métodos mais adequados às suas demandas sociais, tecnológicas, financeiras, políticas e econômicas de combater os Ciberataques.

O que se pode dizer, a partir das interpretações dessa obra é que os combates aos conflitos virtuais não estão restritos à criação de normas jurídicas que orientem um Estado nos procedimentos a serem seguidos para combater e punir a prática de crimes no âmbito virtual.

Para além disso, o combate importa na criação de meios, nas mais variadas áreas de atenção, para que as probabilidades de efetividade aumentem. De nada basta a criação de leis, sem que a sociedade tenha consciência e alcance dos conceitos e elementos que compõe o ciberespaço e o ciberataque.

Em outra dimensão, de nada basta a criação de conceitos e leis, sem meios técnicos que efetivem a busca, no próprio campo virtual, de diligências efetivas para o combate as ações também praticadas no âmbito virtual.

Em um enfoque ainda maior, de nada basta que um Estado adote todos esses meios de proteção, sem o auxílio de outros Estados na efetivação das políticas de prevenção e segurança de forma mútua e conjunta. Isso porque, em concordância com os entendimentos dos autores aqui elucidados, o Ciberataque se trata de uma questão complexa que, por suas características

de não territorialidade e anonimato, há um perpasse rápido e preocupante das ações e dos resultados que envolvem o Ciberataque pela rede mundial de computadores. Tais ações e resultados não se restringem a um espaço físico, a um Estado específico, a um indivíduo delimitado.

Nas palavras do especialista em segurança da informação do Superior Tribunal de Justiça Antonio Horácio Boa Sorte, os riscos estão relacionados principalmente na maneira como o usuário faz uso da tecnologia. Afirma o Desembargador, ainda, que

> *"Obter conhecimento a respeito do assunto ainda é a melhor forma de evitar ser vítima"*.[74]

Dessa forma, a ação que parece mais lógica para o combate dessa nova modalidade de ação no âmbito global é também uma ação complexa, não delimitada a um Estado específico e com esforços conjuntos e mútuos entre os Estados.

Nesse gancho de ideias, e tendo em vista a rapidez que um Ciberataque se demonstra no plano físico, o presente estudo faz compreender que uma forma que se apresenta cabível para o confronto ao Ciberataque é aquela que se apresenta, de igual forma, rápida e efetiva.

No âmbito do direito internacional privado, a cooperação jurídica internacional e, especificamente, o auxílio direto entre os Estados parece se estreitar proximamente a tais características.

Isso porque tal modalidade não prescinde da vinculação do judiciário para a efetivação de providências jurisdicionais ou administrativas . Além disso, no âmbito do ordenamento jurídico brasileiro, a cooperação jurídica internacional não está restrita a um rol taxativo de objetos que podem ser solicitados pelos Estados.

Contrariamente, admite-se o uso de quaisquer diligências judiciais e extrajudiciais que não sejam vedadas pela lei brasileira. Nesse sentido, dispõe o art.27 do CPC:

> *"Art. 27. A cooperação jurídica internacional terá por objeto:*
> *I - citação, intimação e notificação judicial e extrajudicial;*
> *II - colheita de provas e obtenção de informações;*
> *III - homologação e cumprimento de decisão;*
> *IV - concessão de medida judicial de urgência;*
> *V - assistência jurídica internacional;*

[74]Vide:http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/Crimes-pela-internet,-novos-desafios-para-a-jurisprud%C3%AAncia

VI - qualquer outra medida judicial ou extrajudicial não proibida pela lei brasileira."

Em face disso, não se buscou assumir que a cooperação jurídica internacional é a única forma cabível e adequada nessa luta virtual, mas sim adequá-la ao contexto atual como uma possibilidade, diante da escassez de soluções concretas no âmbito técnico e legislativo.

Cabe evidenciar que, diante de Estados com tantas divergências no modo de tratamento de seus direitos, garantias e procedimentos, ainda que a questão do crime virtual e dos Ciberataques se mostre como de extrema relevância para os dias atuais, deve-se sempre levar em conta as especificidades políticas e legislativas de cada Estado ou indivíduo.

Nessa perspectiva, nenhum direito pode ser subsumido em prol de um outro considerado, momentaneamente, mais relevante. Ainda que haja ponderações de princípios, de momentos de conveniência e oportunidade, não admite-se a exclusão de um direito, competência ou jurisdição em prol de outra, por questões de urgência na busca de uma solução.

É nesse sentido, que ainda que diante de ataques, relativizações e mitigações doutrinárias, jurídicas e fáticas, a soberania deve ser preconizada. Sob fundamento de que a urgência, a relevância e a busca incessante pelos Estados no combate ao Ciberataque não justifica a negação ou a não utilização de normas e princípios básicos no âmbito do direito internacional público, nas suas duas faces, internamente, na relação do Estado perante seus indivíduos e, tampouco, na relação externa entre os próprios Estados no convívio na comunidade internacional.

Portanto, faz-se mister ressaltar a importância da disseminação dos novos conceitos que envolvem o combate humano, que não está mais restrito ao plano físico, denotando-se que a guerra cibernética é o novo front de batalha do mundo moderno. Tal problemática é de grande relevância, pois, somente com o fomento do conhecimento nessa área surgirão novas ideias de forma a buscar as melhores soluções para a problemática.

O grande desafio imposto por esse trabalho é justamente formular hipóteses para uma premissa que ainda está em fase de construção. Ou seja, buscar soluções de combate ao fenômeno do Ciberataque que está ainda em fase de evolução na realidade dos Estados.

Ao que parece, majoritariamente, tem-se preferido métodos de cooperação jurídica internacional como forma de retaliação aos Ciberataques, o que nada impede que, diante da dinamicidade da problemática, novas formas legais e legítimas sejam admitidas de forma a otimizar a atuação dos Estados na conquista de um novo espaço. Isso é o que parece mover a

humanidade, o conhecimento e a busca pelos espaços, da terra, para o mar, para o ar, para a lua e, agora, caminhando para o ciberespaço.

6. LEGISLAÇÃO E JURISPRUDÊNCIA

BRASIL. Decreto nº. 4.388 de 25 de setembro de 2002.Promulga o Estatuto de Roma do Tribunal Penal Internacional. Brasília, DF, set 2002.

BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Livro verde: segurança cibernética no Brasil: organização Claudia Canongia e Raphael Mandarino Junior – Brasília: GSCIPR/SE/DSIC, 2010 p.63.

BRASIL. Gabinete de Segurança Institucional. Presidência da República. Portaria nº 45 de 8 de setembro de 2009, do GSI/PR: Disponível em: < http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009 >

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 23 de abril de 2014.

BRASIL. Supremo Tribunal Federal – Súmula Vinculante nº 10.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 2000.

BRASIL Superior Tribunal de Justiça. Resolução nº 9 de 4 de maio de 2005. Dispõe, em caráter transitório, sobre competência acrescida ao Superior Tribunal de Justiça pela Emenda Constitucional nº 45/2004.

BRASIL. Decreto nº. 4.388 de 25 de setembro de 2002.

HABEAS CORPUS nº 147.375 – RJ. Rel. Ministro Jorge Mussi – 5ª Turma STJ. Data de julgamento: 22 de novembro de 2001.

Petição nº 5946 no Agravo Regimental – DF – Rel. Ministro Edson Fachin – 1ª Turma do STF. Data de julgamento: 16 de agosto de 2016.

RECURSO EM HABEAS CORPUS Nº 42.825 – RS. Rel. Ministro Sebastião Reis Júnior – 6ª Turma STJ. Data de Julgamento: 1 de setembro de 2015.

SÃO FRANCISCO. Estatuto da Corte Internacional de Justiça. Carta das Nações Unidas, 1945.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABADE, Denise Neves. Direitos fundamentais na cooperação jurídica internacional: extradição, assistência jurídica, execução de sentença estrangeira e transferência de presos. São Paulo: Saraiva, 2013.

ARAÚJO, Nadia de. Direito Internacional Privado: Teoria e Prática Brasileira. 6 ed. Porto Alegre: Revolução eBook, 2016.

ARAÚJO, Nadia de; GAMA JUNIOR, Lauro. Sentenças estrangeiras e cartas rogatórias: novas perspectivas da cooperação internacional. Disponível na Internet: <http://www.mundojuridico.adv.br/sis_artigos/artigos.asp?codigo=51>.

ARAÚJO, Nádia. Inclusão de regras sobre cooperação jurídica internacional no novo CPC: O novo sistema harmônico brasileiro. Revista Cooperação em pauta. n. 2, março/2015.

ARQUILLA, John; RONFELDT, David, Cyberwar is Coming! (Ed.). In: Athena's Camp: preparing for conflict in the information age. Santa Monica CA: Rand Corp, 1997. (Reedição do artigo originalmente publicado na Comparative Strategy, v. 12, n. 2, 1993)

AZAMBUJA, Darcy. Teoria Geral do Estado. 2 ed. São Paulo: Editora Globo, 2008.

BAKER, K. M. "Soberania". In: FURET, F. Dicionário crítico da Revolução Francesa. Rio de Janeiro: Nova Fronteira, 1989.

BODIN, Jean. Os seis livros da república. Trad. José Carlos Orsi Morel (v. 1)/ José Ignacio Coelho Mendes Neto (vs. 2-6). Rev. José Ignacio Coelho Mendes Neto. São Paulo: Ícone, 2011. (6 v.)

BONAVIDES, Paulo. Ciência Política. 10.ed. São Paulo: Malheiros, 2002.

CASELLA, Paulo Borba; ACCIOLY, Hidelbrando; SILVA, G.E do Nascimento E. Manual de direito internacional público. — 20. ed. — São Paulo : Saraiva, 2012.

CASTELLS, Manuel. Fim do Milênio. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

CHEVALLI ER, Jean Jacques. As grandes obras políticas: de Maquiavel a nossos dias. Tradução de André Praça de Souza Teles .8 ed. Rio de Janeiro: AGIR, 2001.

CLARKE, Richard A.; KNAKER, Robert K. Cyberwar: The Next Threat to National Security and What to Do About It. Tradução: Ramos, Maria Sharlyany MarqueNew York: Ed. Harper Collins, 2010.

DALLARI, Dalmo de Abreu. Elementos de Teoria Geral do Estado. São Paulo: Editora Saraiva. 2 ed. 1997.

FERNANDES, José Pedro Teixeira. Da utopia da sociedade em rede à realidade da sociedade de risco. Análise Social, 207, xlviii (2.º), pp. 260-286. Lisboa, Portugal. 2013.

FREUND, Julien. Sociologia de Max Weber. Trad. Luís Cláudio de Castro e Costa. 2. ed. Rio de Janeiro: Forense, 1975.

GIBSON, W. Neuromancer. Trad. de Alex Antunes (baseada na tradução da 1ª ed. de Maya Sangawa e Silvio Alexandre). 3. ed. São Paulo: Aleph, 2003.

GOLDSMITH, Jack. The Internet and the Legitimacy of Remote Cross-Border Searches. Chicago public law and legal theory working paper no. 16 – Disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=285732

GRINOVER. Ada Pellegrini. Processo penal transnacional: linhas evolutivas e garantias processuais. Revista Brasileira de Ciências Criminais, n.9: São Paulo, 1995.

HOBBES, Thomas. Leviatão, ou, Matéria, forma e poder de um Estado eclesiástico e civil.5 ed. São Paulo: Martil Claret, 2011.

KOHONA,P.T.B. The United NationsTreatyon The Internet. The American Journal of International Law, Vol.92, nº1, 2009. Disponível em:<http://www.jstore.org/stable/2998074>

LEÃO, Lucia. Derivas: cartografias do ciberespaço. São Paulo. Annablume, 2004.

LÉVY, Pierre, Qu'est-ce que le virtuel?.Paris, Éditions La Découverte, coll. Sciences et Sociéte, 1995.

LISBOA. Instituto Nacional da Defesa Nacional. Estratégia da Informação e Segurança no Ciberespaço nº 12. Lisboa: Cadernos do IDN, 2013.

LOCKE, John. Dois tratados sobre o Governo. Tradução de Julio Fischer. São Paulo: Martins Fontes, 2005.

MADRUGA, Antenor, FELDENS, Luciano. Dados eletrônicos e cooperação internacional: limites jurisdicionais. Temas de cooperação internacional / Secretaria de Cooperação Internacional. Brasília:MPF,2015.

MATSUYAMA, K. G.; LIMA, J. A. A. Crimes cibernéticos: atipicidade dos delitos. Disponível em:
<http://www.cedipe.com.br/3cbpj/docs/artigos_pdf/11_crimes_ciberneticos_atipicidade_dos_delitos.pdf.>

MIRANDA, Napoleão. Globalização, Soberania Nacional e Direito Internacional. Brasília: R. CEJ, n.27, Out-Dez/.2004.

MIRANDA. Jorge. Teoria do Estado e da Constituição. Rio de Janeiro: Fonrense, 2005.

MOREIRA, João Manuel Dias. O impacto do ciberespaço como nova dimensão nos conflitos. Lisboa: Boletim Ensino. Investigação nº 13, 2012.

MUELLER, M.L. The Global Politics of Internet Governance. Cambridge: The MIT Press. Massachusetts Institute of Technology, 2010. Disponível em: <http://pages.uoregon.edu/koopman/courses_readings/phil123-net/intro/mueller_networksand-states.pdf>.

NADER, Paulo. Introdução ao estudo do direito. 36 ed. Rio de Janeiro: Forense, 2014.

NYE, Joseph S. Cyber Power. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010. Disponível em: < http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf >

OTAVIO, Rodrigo, Direito Internacional Privado, Parte Geral, Rio de Janeiro, Ed. Freitas Bastos, 1942.

PIRES, H.F. Estados Nacionais, Soberania e Regulação da Internet. Barcelona: Revista Eletrônica de Geografia y Ciencias Sociales, v.XVI, n.418, Nov/2012. Disponível em: < http://www.ub.edu/geocrit/coloquio2012/actas/12-H-Pires.pdf. >.

REZEK, José Francisco. Direito internacional público: curso elementar – 11 ed. ver e atual – São Paulo: Saraiva, 2008.

ROUSSEAU. Do contrato social. São Paulo: Martin Claret, 2003.

SHACKELFORD, Scott J. From nuclear war to net war: analogizing cyber attacks in international law. Berkeley Journal of International Law. v. 27, n. 2009. Disponível em: <http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7>.

SILVA, Ricardo Perlingeiro Mendes da Silva. O direito internacional contemporâneo – estudos em homenagem ao professor Jacob Dolinger. Rio de Janeiro: Renovar, 2006.

SKINNER, Quentin. The Foundations of Modern Political Thought, vol.2: The Age of Reformation, 19th printing, Cambridge: Cambridge University Press, 2013.

STORY, Joseph. Comentaries on the Conflict of Laws Foreign and Domestic, In Regard to Contracts, Rights and Remedies, And Especially in Regard to Marriages, Divorces, Wills, Successions and Judgments. 2 ed. Little, Brown: 1841.

STRECK, Lenio Luiz; MORAIS, Jose Luis Bolzan de. Ciência Política & Teoria do Estado. 8 ed. São Paulo: Editora Livraria do Advogado, 2013.

THIERRY, Humber. L'évolution du droit international: cours général de droit international public. Paris: RCADI, 1990.

WEBBER, Patrícia Maria Núñez. Cooperação internacional penal: conceitos básicos. Temas de Cooperação Internacional / Secretaria de Cooperação Internacional – Brasília: MPF, 2015.

WEBER, Max. "A política como vocação". in M. Weber, Ciência e política: duas vocações. Tradução de Jean Melville. São Paulo: Martin Claret, 2003.

WEBER, Max. Economia e sociedade. Brasília: Editora UNB, 1991.