ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR

CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA – ASCES/UNITA

BACHARELADO EM DIREITO

JOHANA KYVIA CHAVES BRITO

LETÍCIA MARIA DOURADO LEITE

MARIA BEATRIZ MUNIZ BRAZ DA SILVA

O QUINTO DOMÍNIO: Os Princípios da Dignidade da Pessoa Humana e do Direito Humanitário de Guerra em face da Guerra Cibernética

CARUARU

2023

JOHANA KYVIA CHAVES BRITO

LETÍCIA MARIA DOURADO LEITE

MARIA BEATRIZ MUNIZ BRAZ DA SILVA

O QUINTO DOMÍNIO: Os Princípios da Dignidade da Pessoa Humana e do Direito Humanitário de Guerra em face da Guerra Cibernética

Trabalho de Conclusão de Curso apresentado à Bancade TCC do Centro Universitário Tabosa de Almeida (Asces-Unita), como requisito parcial à aprovação nocurso de Bacharelado em Direito.
Orientador: **Professor Doutor Emerson Francisco de Assis**.

CARUARU

2023

RESUMO

O presente projeto pretende expor, por meio dametodologia de estudo indutivo, pela pesquisa bibliográfica e documental, uma definição abrangente quanto o fenômeno da “nova modalidade de Guerra”, a chamada Guerra Cibernética. Através de um alicerce teórico e demonstrando a incidência e ausência de limites, este artigo objetiva apresentar a relevância da normatização legislativa do tema no âmbito nacional e internacional. Para isso, frente à importância da Dignidade da Pessoa Humana em meio ao conflito de leis no espaço-tempo e o (insuficiente) amparo dos Direitos Humanos, Direito Internacional Privado e Público quanto à essa normatização, se faz necessário, com o propósito de fundamentar a regularização da Guerra Cibernética, explorar a sua gama de definições, pesquisando, assim, sobre seus princípios, características e particularidades.

Palavras-Chave: Guerra Cibernética. Direitos Humanos. Direito Internacional Digital. Dignidade da Pessoa Humana. Direito Internacional Humanitário.

ABSTRACT

The current project intends to expose, through the methodology of the inductive study and bibliographic and documentary research, a comprehensive definition of the phenomenon of a "new kind of warfare" called Cyber Warfare. Through a theoretical foundation and demonstrating the incidence and absence of limits, this dissertation aims to present the relevance of the legislative normalization of the theme in the national and international spheres. For this, given the importance of the Dignity of the Human Person amid the conflict of laws in space-time and the (insufficient) support of Human Rights, Private and Public International Law regarding this normalization, it is necessary to ground the regulation of Cyber War, explore its range of definitions, thus researching on its principles, characteristics, and particularities.

Keywords: Cyberwar. HumanRights. International Digital Law. Dignity of theHuman Person. InternationalHumanitarian Law.

SUMÁRIO

1. INTRODUÇÃO 5

2. O DIREITO HUMANITÁRIO DE GUERRA E O PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA 6

2.1 Direito Humanitário de Guerra: Conceito e Contexto Histórico 6

2.2O conceito do Princípio da Dignidade da Pessoa Humana 8

2.3 Principais normas do Direito Humanitário de Guerra 9

3. CONSIDERAÇÕES SOBRE A ASCENSÃO DA SOCIEDADE CIBERNÉTICA 11

3.1 A Revolução da Tecnologia da Informação 11

3.2 O contexto social que está inserido a dinâmica da mudança tecnológica 13

3.3A autoridade da Ordem Pública Internacional na *internet* 14

4. GUERRA CIBERNÉTICA: ASPECTOS GERAIS 15

4.1 Guerra Cibernética: Conceito e Contexto histórico **15**

4.2Emprego da Guerra Cibernética: Campos de atuação e análise de casos concretos **17**

5. A GUERRA CIBERNÉTICA EM FACE À SUA ESCASSEZ NORMATIVA 19

5.1 A necessidade de regulamentação da Ciberguerra **Erro! Indicador não definido.**

5.2A intervenção do Conselho de Segurança das Nações Unidas para regulamentação da Guerra Cibernética frente à necessidade de criação de Tratados Internacionais 21

6. CONSIDERAÇÕES FINAIS 22

REFERÊNCIAS 24

1. INTRODUÇÃO

Desde a Segunda Guerra Mundial, em especial após os resultados provenientes da Primeira Guerra do Golfo (Operação Tempestade no Deserto), é notório as mudanças significativas nas chamadas “espécies de guerra”.

Atualmente, com a predominância da *internet* e da tecnologia, bem como frente à inevitável evolução histórica, é plausível destacar que vem se enrustindo na sociedade uma inovadora corrente doutrinária que disserta sobre as “novas modalidades de guerra” pautando, em suas teses, uma perspectiva mais pacificadora e inovadora dos Estados, haja vista a adoção, no âmbito internacional, das normas inerentes ao *jus in bellum*.

Trata-se, portanto, da predominância do virtual caracterizada por uma governança de dados e gestão da informação digital, elementos estes predominantespara uma nova modalidade de controle social, qual seja o chamado "Quinto Domínio", externado pela Ciberguerra, um desdobramento da Guerra Assimétrica.

O termo "Quinto Domínio" surge diante do cenário de difusão e evolução das tecnologias, ao qual a sociedade em geral está integralizada ao ciberespaço. Tal expressão agrega uma nova configuração de conflito aos campos de guerra convencionais: Espacial, Aéreo, Marítimo e Terrestre (CAMPOS, 2014).

Nas palavras de Parks e Duggan (2001), o mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes, existindo, desta forma, diversos mundos cibernéticos, sendo a *internet* e as redes a elas relacionadas, o mais relevante para a Guerra Cibernética.

Em suma, esse fenômeno consiste uma nova configuração de guerra (mais difícil de se combater por meio das forças convencionais), pautada na tecnologia e com novos atores (não necessariamente estatais), objetivando o domínio Espacial, Aéreo, Marítimo e Terrestre. Noutros termos, o conflito cibernético é diferente, principalmente quando se trata de espaço.

Logo, com a globalização e com a avanço da tecnologia, conclui-se que esse novo desdobramento de guerra assimétrica transforma a maneira como as sociedades modernas se inter-relacionam se fazendo necessário, deste

modo, uma nova visão para o Direito, no qual se assegure a utilidade prática do convívio e se resguarde os limites da vida em sociedade, para assim não ferir Princípios Constitucionais, tal qual o da Dignidade da Pessoa Humana.

Desta feira, tomando-se como pressuposto que está "anarquia internacional"(externada pelo não reconhecimento da Ciberguerra como uma guerra legitimada pela ordem jurídica internacional)acarretará mudanças sociais econsequentes conflitos de leis que serão (é) um dos maiores desafios da Sociedade Digital, o presente artigo busca, através de uma metodologia de estudo indutivo a da pesquisa bibliográfica e documental,recobrar-se como as regras de Direito Internacional aplicadas às características, conceitos e princípios da guerra tradicional coexistem em relação a esse "quinto domínio" regido pela Internet e voltado ao campo cibernético.

2. O DIREITO HUMANITÁRIO DE GUERRA E O PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA

2.1 Direito Humanitário de Guerra: Conceito e Contexto Histórico

O Direito Internacional Humanitário (DIH), também chamado de “Direito de Guerra” ou “Direito ao Conflito Armado”, diz respeito à proteção à vida, à saúde e à dignidade, e consiste em um conjunto de normas do Direito Internacional Público que atua de forma a regular as condutas e limitar os efeitos durante a ocorrência de conflitos armados (JOBIM, 2021).

É notório que, desde os primórdios da civilização, é fator inerente à construção social a ocorrência de conflitos na convivência entre os seres humanos. Acontece que, conforme observado no contexto cultural e social no qual estamos inseridos e consoante aos ensinamos de Clausewitz (2003), a maioria destes conflitos entre os povos são violentos e armados, excepcionalmente se resolvendo por meios humanitários e pacíficos:

> Não comecemos por uma definição de guerra, difícil e pedante; limitemo-nos a sua essência, ao duelo. A guerra nada mais é que um duelo em uma escala mais vasta. Se quisermos reunir num só conceito os inumeráveis duelos particulares de que a guerra se compõe, faríamos bem em pensar na imagem de dois lutadores. Cada um tenta, por meio de sua força física, submeter o outro a sua vontade; seu objetivo imediato é abater

> o adversário a fim de torná-lo incapaz de toda e qualquer resistência. A guerra é um ato de violência destinado a forçar o adversário a submeter-se a nossa vontade. (CLAUSEWITZ, 2003, p. 07)

Nesse ínterim, surge o Direito Internacional Humanitário, visando restringir os meios e métodos adotados na Guerra, de forma a limitar suas consequências e proteger aqueles que não participam ativamente dos conflitos. O DIH começa a ser aplicado na ocorrência de qualquer espécie de conflito armado, internacional ou não internacional, haja vista que, através da adesão ou ratificação de Tratados e Convenções Internacionais, objetiva criar normas para regular as relações de Estado de modo que os conflitos armados sejam os mais pacíficos possíveis (COMITÊ INTERNACIONAL DA CRUZ VERMELHA, 1998).

Portanto, como pressuposto desse conceito criado a partir do Direito Internacional Público, originou-se a ideia do binômio “Guerra e Paz”, desenvolvida com base entre o chamado “Direito de Paz” e “Direito de Guerra”. O “Direito de Paz” seria aquele que regeria as relações internacionais em tempos de paz, enquanto o “Direito de Guerra” seria a exceção, regendo as relações internacionais durante os conflitos bélicos (NARDO, 2017).

Segundo Sassóli (NARDO, 2017 *apud* SASSOLI, 2019) seria necessário, no conceito de “Direito de Guerra”, fazer uma subdivisão quanto à legitimidade (*jus ad bellum*) e às formas de condução (*jus in bello*) dos conflitos armados. O *jus ad bellum* consistiria no direito de fazer guerra pautado em determinadas justificativas, enquanto o *jus ad bello*, mais conhecido como “Direito Humanitário”, consistiria em mitigar os sofrimentos decorrentes dos conflitos bélicos.

Nesse contexto, visando a plena eficácia dos princípios decorrentes do DIH, os Estados passam a ter o dever de aprovar legislações e adotar medidas práticas para que as normas provenientes do *jus in bello* sejam plenamente efetivas. Sendo inserido, frente à essa necessidade, uma fundamentação legal pautada em Tratados, Convenções, Protocolos e Costumes aceitos universalmente, destacada, em especial, pela criação da Cruz Vermelha, da Convenção de Genebra (em vigor desde 1950 e atualmente ratificada por 194 países), das regras do “Direito Internacional Consuetudinário” e do Conselho

de Segurança das Nações Unidas, diretrizes adotadas por todos os Estados (NARDO, 2017; CICV, 1998).

2.2 O conceito do Princípio da Dignidade da Pessoa Humana

O fundamento para o entendimento do Princípio da Dignidade da Pessoa Humana é constituído pelos Direitos Humanos, como direito histórico de um sistema moralista que procedeu fortemente durante o século XX, quando se iniciou a internacionalização da Liga das Nações, da Organização Internacional do Trabalho, dentre as variadas organizações que permitiram a aderência legítima dos Direitos Humanos que, quando transformado e melhorado durante os anos, redefiniram o significado da Moral para um *status* do Direito como objeto realmente humanitário. Sua ressignificação veio com a medida integral de dar limites ao Estado e sua liberdade quando se tratava do papel do indivíduo em sociedade (PIOVESAN, 2021).

Eventualmente, quando concebido por Bobbio, os Direitos Humanos já fortalecidos formaram determinadas quatro gerações:

> 1ª Geração: Direitos Individuais – pressupõem a igualdade formal perante a lei e consideram o sujeito abstratamente; 2ª Geração: Direitos Coletivos – os direitos sociais, nos quais o sujeito de direito é visto no contexto social, ou seja, analisado em uma situação concreta; 3ª Geração: Direitos dos Povos ou os Direitos de Solidariedade: os direitos transindividuais, também chamados direitos coletivos e difusos, e que basicamente compreendem os direitos do consumidor e os relacionados à questão ecológica; 4ª Geração: Direitos de Manipulação Genética – relacionados à biotecnologia e bioengenharia, tratam de questões sobre a vida e a morte e requerem uma discussão ética prévia (BOBBIO, 1992, p.6).

Tal multiplicidade do Direito Humano, como instrumento, surgiu de uma evolução destinada a pessoa humana, para que esta não fosse estranha a rotina normativa da prática da jurisdição Internacional que tem como princípio o pacto democrático entre a sociedade e seu governo, assim mudando o comportamento dos Estados quando, reconhecendo a pessoa humana como parte não só de um mecanismo, mas como ser autônomo que evidencia segurança própria e é independente de ordens permissivas, uma vez que a

Constituição de sua nação deixaria expresso seus Direitos, finalmente validando na prática sua dignidade humana (PIOVESAN,2021).

A segurança individual é determinada pelo Direito Internacional como consta os tratados e preceitos consuetudinários expressos. Indo além da 1° geração, a Dignidade da Pessoa Humana estabelece o homem individualmente, não só como parte de um coletivo, mas ultrapassando a abstração em que se fixam as leis (SARLET; SARLET; BITTAR, 2015).

O conceito do Princípio da Dignidade da Pessoa Humana reitera com uma nova interpretação que permite a pessoa se colocar em prioridade concreta como personalidade individual sobre os interesses da comunidade. Logo, isso representa a manutenção da dignidade individual acima da soberania do Estado para respeitar a inclusão do princípio, e tal ato não exonera o Estado, já que preservar a dignidade é validar a essência do pacto social ao não admitir que sua Nação viole a Dignidade da Pessoa Humana, assim, determinando eficácia ao princípio como direito fundamental (SARLET; SARLET; BITTAR, 2015).

2.3 Principais normas do Direito Humanitário de Guerra

Ao passo que os Direitos Humanos, instituídos através da Declaração Universal dos Direitos Humanos de 1948, tutelam os direitos fundamentais perante o Estado - tratando da relação Estado-Indivíduo -, os Direitos Internacionais Humanitários (DIH) trabalham a relação Estado-Estado em situação de conflito armado, tutelando sobre as regras pertinentes à forma de condução do *jus in bello*. Ambos institutos, não obstante, trabalham o respeito à integridade física e moral da população (NARDO, 2017).

O Direito Internacional Humanitário é o conjunto de normas internacionais, de origem convencional ou consuetudinária, especificamente destinado a ser aplicado nos conflitos armados, internacionais ou não internacionais, e que limita, por razões humanitárias, o direito das partes em conflito de escolher livremente os métodos e os meios utilizados na guerra, ou que protege as pessoas e os bens afetados, ou que possam ser afetados pelo conflito (SWINARSKI, 1996).

Outrossim, como já abordado, o Direito de Guerra é um instituto composto por diversas normas que, por questões humanitárias, buscam limitar os efeitos dos conflitos armados, protegendo indivíduos que não são, ou não são mais, participantes nas hostilidades, restringindo os métodos e meios durante as guerras (NARDO, 2017).

A busca do equilíbrio entre o humanitarismo e a necessidade militar é a filosofia central do DIH, balanceando a proporcionalidade da demanda militar no cálculo dos danos potenciais dos ataques aos civis, limitando e avaliando o cumprimento da missão seguindo os conformes das exigências impostas pelos princípios de caráter humanitário (ICRC, 2010).

Por conseguinte, a filosofia desse instituto é perceptível em seus fundamentos básicos, todos possuindo caráter preventivo, frisando a segurança dos civis inseridos nesses ambientes delicados. Os principais fundamentos que norteiam as regras contidas no Direito Humanitário de Guerra a serem aplicadas nos períodos de hostilidade envolvem a humanidade - reprimindo ações de destruição que não sejam de objetivo militar de caráter legítimo -, a necessidade militar, a distinção entre civis e combatentes - levando em consideração que os ataques nunca devem ser dirigidos contra civis, apenas contra combatentes -, a proporcionalidade e a precaução - tomando todas as precauções viáveis para evitar, e em qualquer caso minimizar, qualquer dano aos civis (SASSÒLI, 2019).

Em suma, as necessidades militares não podem configurar justificativa de condutas desumanas, devendo sempre fazer o uso da proporcionalidade à vantagem militar concreta e direta, extinguindo ações que causem sofrimento desnecessário aos civis, bem como aos seus bens, que não podem ser objetos de ataques ou represálias (CICV, 1998).

As regras fundamentais do DIH, incluídas nas Convenções de Genebra (1949) juntamente com os Protocolos Adicionais, são juridicamente obrigatórias para todos os Estados que os ratificaram. Tais normas que compõem o referido regimento foram decididas através de tratados universalmente ratificados, como a Convenção de Genebra de 1949 - ratificado em 196 países -, e as leis de direito internacional já vigentes (CICV, 1998). Existem 7 principais regras que são consideradas as normas imprescindíveis do Direito Internacional Humanitário:

> 01) As pessoas fora de combate e aqueles que não participam diretamente das hostilidades têm direito ao respeito à vida e à integridade moral e física. Devem, em qualquer circunstância, ser protegidos e tratados com humanidade sem nenhuma distinção adversa.
> 02) É proibido matar ou ferir um inimigo que tenha se rendido ou que esteja fora de combate.
> 03) Os feridos e os doentes devem ser recolhidos e tratados pela parte do conflito que os têm em seu poder. A proteção também abrange a equipe médica e os estabelecimentos, o transporte e os equipamentos médicos. O símbolo da Cruz Vermelha e o do Crescente Vermelho são o sinal desta proteção e devem ser respeitados.
> 04) Os combatentes capturados e os civis sob a autoridade de uma parte inimiga têm direito ao respeito pela vida, dignidade, direitos e convicções pessoais. Devem ser protegidos contra todos os atos de violência e represálias. Devem ter o direito de se corresponder com suas famílias e de receber socorro.
> 05) Todos devem ter direito de se beneficiar com as garantias judiciais fundamentais. Ninguém pode ser responsável por um ato que não cometeu. Ninguém deve ser submetido à tortura física ou mental, ao castigo corporal ou ao tratamento cruel ou degra dante.
> 06) As partes do conflito e os membros de suas forças armadas não têm opções ilimitadas de métodos e meios de guerra. É proibido utilizar armas ou métodos de guerra que causem perdas desnecessárias ou sofrimento excessivo.
> 07) As partes do conflito sempre devem distinguir entre população civil e combatentes, a fim de poupar a população civil e seus bens. Nem a população civil nem as pessoas civis devem ser alvo de ataque. Os ataques devem ser dirigidos apenas contra objetivos militares. (CICV, 1998)

Importante ressaltar que na hipótese de infração dessas normas de guerra, os casos são documentados e investigados pelos Estados ou tribunais internacionais, este último que atuará com o objetivo de complementar as decisões tomadas nos tribunais dos Estados-partes nas presunções de parcialidade ou inidoneidade (NARDO, 2017 *apud* SASSÒLI, 2019).

3. CONSIDERAÇÕES SOBRE A ASCENSÃO DA SOCIEDADE CIBERNÉTICA

3.1 A Revolução da Tecnologia da Informação

Entre as décadas de 1950 e 1970, com o domínio das indústrias e com o advento das diversas descobertas e evoluções no campo tecnológico surge, no contexto da Guerra Fria, a denominada “Revolução Técnico-Científico-

Informacional” ou “Terceira Revolução Industrial”, caracterizada (principalmente) por uma série de alterações políticas, sociais e econômicas (FREITAS, 2022).

É certo que, diferentemente de qualquer outra revolução já existente, a chamada “Revolução da Tecnologia da Informação” tem como âmago - haja vista a predominância dos mecanismos tecnológicos -, a tecnologia da informação, o processamento e a comunicação, ocasionando, desta forma, um novo paradigma tecnológico (CASTELLS, 1999).

Nesse cenário, frente ao surgimento dos novos meios de comunicação e de transmissão de informações, a população mundial se encontrou inserida em um ambiente de transformação, vivenciando, desta forma, um novo contexto social (globalizado e capitalista), havendo, massivamente, a substituição da "cultura material" pela “virtual” (CASTELLS, 1999, p. 498):

> Redes são instrumentos apropriados para: a economia capitalista baseada na inovação, globalização e concentração descentralizada; para o trabalho, trabalhadores e empresas voltadas para a flexibilidade e adaptabilidade; para uma cultura de desconstrução e reconstrução contínuas.

Nesse ínterim, constata-se que, como uma tendência histórica, as redes e a evolução tecnológica da informação constituem:

> [...] a nova morfologia social de nossa sociedade e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura. [...] é um instrumento apropriado para a economia capitalista voltada para a inovação, globalização e concentração descentralizada; para o trabalho, trabalhadores e empresas voltadas para a flexibilidade e adaptalidade; para uma cultura de descontrução e reconstrução contínuas; para uma política destinada ao processamento instantâneo de novos valores e humores públicos; e para uma organização social que vise a suplantação do espaço e invalidação do tempo (CASTELLS, 1999).

Se torna indiscutível, portanto, a afirmação de que com a predominância dos mecanismos tecnológicos - os quais podem ser diretamente representados por meio da *internet,* robótica, telecomunicações e informática -, vigora um novo paradigma tecnológico que se organiza em torno da tecnologia da informação, paradigma este que é compreendido através do processamento e

aplicação obtidas através do uso e das informações obtidas por meio do uso da tecnologia e das telecomunicações (CASTELLS, 1999).

3.2 O contexto social que está inserido a dinâmica da mudança tecnológica

Noção de direitos inerentes à pessoa humana encontra expressão, ao longo da história, de maneiras e lugares distintos. E, o progresso dos meios digitais no espaço comum e no ciberespaço está sendo uma constante, evoluindo conforme o que a atualidade necessita com procedimentos infindáveis, assim, exigindo-se infinitos aprimoramentos de segurança.

Diante disso, observam-se crises geopolíticas e sociais ligadas ao avanço tecnológico, uma vez que o direito não consegue acompanhar as inseguranças individuais dos usuários, sendo lesões silenciosas e violentas atacando os direitos humanos, tal fato criando uma patologia social de irracionalidade que, com o avanço da mídia e seus perfis é desintegrada a racionalidade natural quando há interação humana, dita Eduardo Bittar, Ingo Sarlet e Gabrielle Sarlet (2022, p. 15):

> A era digital se caracteriza por uma combinação de aceleração e tecnologia, que são responsáveis por afetar todas as demais dimensões da vida humana. Na era digital, a tecnologização das interações sociais, o condicionamento robótico das ações sociais e a desumanização das relações humanas arriscam o horizonte do futuro na direção do desprezo à dignidade humana. Em estudo anterior foi possível definir a emergência deste novo modelo de sociedade - nos termos de uma sociedade digito-cêntrica -, conceito este que é aqui invocado para nominar o conjunto das transformações nas sociedades contemporâneas, digitalizadas e hipertecnológicas. Nela, o horizonte do futuro passa a se fundir com o horizonte do presente. Aliás, é isto que faz da era digital a nova fronteira da modernidade, enquanto se inscreve, no horizonte do presente a vitória do tempo sobre o espaço.

A era digital, além de benefícios, vem aumentando os riscos quando se trata da dimensão das interações humanas e seus interesses, que são instantâneos e diretos frente à sociedade, assim, tem como resultado o efêmero como novo modo de produção nas relações humanas. Em campo digital, as pessoas se tornam fluidas, reduzidas a perfis projetados, quando

definem várias verdades sobre si e, ainda, seus dados pessoais (BAUMAN, 2001).

A intensidade que há na superfluidez da informação e o seu proveito adverte em que grau de importância que está a Dignidade da Pessoa Humana, atualmente, quando comparada a força dos efeitos da máquina sobre os efeitos do homem, assim, desrespeitando a humanidade no ambiente digital, com a propagação de condutas antissociais e permissões fazendo com que a opressão se aloje em todas as dimensões, seja ela anônima ou não, na hipercodificação os meios usados para tornar o ambiente favorável para justiça não são efetivos (CASTELLS,1999).

3.3 A autoridade da Ordem Pública Internacional na *internet*

Tendo em vista que a estruturação proposta no conceito de “ordem pública” contém valores essenciais relativos ao ordenamento jurídico - os quais são de suma importância no exercício do Poder Judiciário -, pode-se dizer que a prerrogativa do mesmo possui o poder necessário para atuar na resolução dos conflitos surgidos na Internet (CAMPOS NETO, 2014).

Em contrapartida, a “ordem pública” no Direito Internacional Privado inibe a aplicabilidade das leis estrangeiras, o reconhecimento de atos realizados no exterior e a execução de sentenças proferidas por tribunais de outros países, visando buscar a preservação da soberania nacional de cada país. Por esse motivo, quando tal princípio é levado para a área do Direito Digital sem uma certa adaptação, somando com o vácuo de uma autoridade central, casos conflituosos cibernéticos ficam à mercê da cooperação entre os países para serem devidamente resolvidas (PINHEIRO, 2016).

Prepondera uma tensão no campo cibernético motivada pela intenção individual de cada Estado em regular um fenômeno global com uma perspectiva exclusivamente local, ou seja, sob um eixo particularista (MOORE, 2004).

Ao pôr em análise as noções dos eixos de universalismo e de particularismo em cima de casos práticos envolvendo o mundo cibernético, chega-se à conclusão de que, assim como leciona Jacob Dolinger (2021), o ato de procurar soluções para os conflitos internacionais através de Convenções e

Tratados como propõe a abordagem do método universalista apresenta-se como a mais apropriada e com maiores chances de eficiência para funcionar nas resoluções de conflitos cibernéticos, e não aplicando as normas do direito positivo interno nas relações privadas no plano internacional, como preconiza o método particularista.

Dessa forma, torna-se perceptível que dentro dos maiores desafios da Sociedade Digital está a resolução de conflitos de leis no espaço, levando em consideração os fatores de globalização e “aterritorialismo”. Destarte, a ideia de uma ordem pública internacional digital - atribuindo uma jurisdição própria para a Internet -, mostra-se como a melhor solução para cessar os debates sobre a aplicação do direito estrangeiro *versus lex fori* (lei do foro), levando em conta que recorrer ao critério territorial para a indicação da norma a ser aplicada mostra-se ineficaz aos casos práticos recorrentes no campo cibernético (SOARES;RIBEIRO, 2017).

4. GUERRA CIBERNÉTICA: ASPECTOS GERAIS

4.1 Guerra Cibernética: Conceito e Contexto histórico

Antes de adentrarmos, efetivamente, à compreensão sobre o que se trata essa nova cultura, externada pela Revolução Cibernética ou, como é comumente chamada, a “Guerra Cibernética” ou “Ciberguerra”, se faz importante compreender alguns conceitos iniciais a respeito deste tema, a exemplos do contexto histórico-cultural em que a Ciberguerra está inserida e, até mesmo, o próprio conceito de “guerra” e de “cibernética”.

O *website* Dicio - Dicionário Online de Português (2022), cita que “guerra”, dentre seus variados conceitos, pode ser entendida como: “Conflito armado entre povos ou etnias diferentes, buscando impor algo pela força e pela violência, com o objetivo de proteger seus próprios interesses” [...] “qualquer luta sem armas: guerra ideológica, religiosa” (DICIO - DICIONÁRIO ONLINE DE PORTUGUÊS, 2022).

No mesmo sentido, Mazzuoli (2021, p.1024) conceitua a "Guerra" como:

> [...] todo conflito armado entre dois ou mais Estados, durante um certo período de tempo e sob a direção dos seus respectivos governos, com a finalidade de forçar um dos

> adversários a satisfazer a(s) vontade(s) do(s) outro(s). Ela normalmente se inicia com uma declaração formal de guerra e termina com a conclusão de um Tratado de Paz, ou outro ato capaz de pôr termo às hostilidades e findá-la por completo. [...] Para além do seu caráter estritamente formal (assim entendida a guerra que é formalmente declarada), a guerra também pode ser entendida num sentido material, quando apesar de não se ter formalmente declarado o início das hostilidades, tem-se início o uso da força armada por um Estado dirigido contra outro (ou outros) com a finalidade de impor a este (ou estes) a sua única e exclusiva vontade.

Em contrapartida, relacionado à definição de “cibernética” não há um conceito delimitado e bem consolidado, haja vista que nesta definição existem diferentes tendências e teorias. Entretanto, para o tema em questão, se faz importante destacar a etimologia e a utilização da palavra como adjetivo, previstas no *website* Dicio - Dicionário Online de Português (2022), quais sejam, respectivamente: "[...] a uma arte que tende a representar, utilizando os recursos da técnica moderna, coisas em movimento; cinética." e "A palavra cibernética deriva do inglês cybernetics, do grego “kubernētiké”, que significa arte de dirigir, governar." (DICIO - DICIONÁRIO ONLINE DE PORTUGUÊS, 2022).

Nesse interim, conclui-se, conforme se extrai do Portal São Francisco (2022), que a cibernética: “[...] não trata das coisas, mas formas de comportamento [...]” tendo, portanto, “[...] como domínio o desenho ou descoberta e aplicação de princípios de regulação e comunicação” (PORTAL SÃO FRANCISCO, 2022).

Nota-se, ainda, que essa concepção sempre esteve presente na sociedade estando também, gradativamente, evoluindo, haja vista que a origem da cibernética ocorreu, conforme argumenta Viviane Hengler Corrêa Chaves (2010), no ápice das necessidades provenientes da Segunda Guerra Mundial sendo consolidada:

> [...] nas experiências de guerra de Norbert Wiener e Julian Bigelow. Os computadores ajudaram-na a representar o mundo nas máquinas, e mudaram, de forma significativa, a ideia que o homem tinha sobre a tecnologia dos computadores. O desenvolvimento da Cibernética levou os cientistas a novos modelos matemáticos, cada vez mais complexos, decorrentes de novas formas de conceber o envolvimento sistêmico homem-máquina. Termos comuns no mundo contemporâneo, tais como cyborg, ciberespaço, cibercultura entre outros têm a mesma origem embrionária, a qual abriu caminhos para uma

> ampla gama de possíveis desdobramentos. Destaca-se o fato de que ao contexto e as necessidades surgidas com a Segunda Guerra Mundial propiciaram o ambiente para o desenvolvimento desse conhecimento de cunho interdisciplinar, que culminaram na origem da Cibernética. Foram criados grupos multidisciplinares compostos de matemáticos, físicos, engenheiros, cientistas sociais, e outros, que, em conjunto, aliavam a força de seus conhecimentos para resolver os problemas de esforço de guerra.

Nesse ínterim, podemos observar, através da análise da evolução histórica do conceito de guerra, que esse "novo cenário de guerra", qual seja a "Ciberguerra", pode ser entendida como um desdobramento da 4ª Geração da Guerra ou da chamada Guerra Assimétrica, sendo, portanto, resultado de uma evolução política, social, econômica e tecnológica, proveniente desde o século XX, que, por extrapolar os limites do espaço nacional, haja vista ser pautada em tecnologia e por ter como sujeito ativo agente atores não-estatais, transformou a maneira como as sociedades modernas se inter-relacionam.

4.2 Emprego da Guerra Cibernética: Campos de atuação e análise de casos concretos

Reforçada a conceituação do termo Guerra Cibernética, disposto no glossário das Forças Armadas há a seguinte definição:

> Uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. (BRASIL, 2014)

Em um cenário de Guerra Cibernética, existem diversos campos de atuação, os quais podem ser realizados os ataques (BRASIL, 2017). As possibilidades de suas ações incluem:

> 2.6.1 São possibilidades da guerra cibernética:
> a) atuar no espaço cibernético, por meio de ações ofensivas, defensivas e exploratórias;
> b) cooperar na produção do conhecimento de inteligência por meio dos dados obtidos na fonte cibernética;
> c) atingir sistemas de informação de um oponente sem limitação de alcance físico e exposição de tropa;
> d) cooperar com a segurança cibernética, inclusive de órgãos externos ao Ministério da Defesa, mediante solicitação ou no contexto de uma operação;

> e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da guerra cibernética;
> f) facilitar a obtenção da surpresa, com base na exploração das vulnerabilidades dos sistemas de informação do oponente;
> g) realizar ações contra oponentes com poder de combate superior; e
> h) realizar ações com custos significativamente menores do que aqueles envolvidos nas operações militares nos demais domínios. (BRASIL, 2017)

Nesse sentido, sendo o objetivo principal comprometer as ações da(s) nação(ões) adversária(s), a nação autora dos ataques irá planejá-los visando os alvos estratégicos previamente estabelecidos, fazendo uso de uma força especializada na área tecnológica, os hackers (BRASIL, 2017).

A princípio, a dificuldade está em diversos aspectos doutrinários sobre a Guerra Cibernética ainda está em debate no comando do Exército. Por ser algo recente as discussões sobre esse quinto domínio, ambiente cibernético, que permeia todos os demais domínios os apresentando uma vasta pesquisa para batalha em determinado território que qualquer outra força militar não tem acesso, haja vista não se encaixar nos âmbitos de guerra convencionais (terrestre, marítimo, aéreo e geoespacial). Visto que, o próprio manual quanto a Guerra Cibernética, teve a sua primeira versão publicada há cinco anos atrás no Brasil, além de existirem poucos especialistas militares que tem exercício no mundo virtual. O CIGE (Centro de Instrução de Guerra Eletrônica), órgão gestor e formador dos recursos humanos para atuação cibernética, formou uma turma de militares ainda em 2012 (BOMBASSARO, 2018).

O conhecimento cibernético é em grande parte técnico e exige prática constante, sobrevivendo com o esforço na política de reter mais pessoas capacitadas na área citada. De maneira que, atualmente é urgente tal integração, com a visível guerra entra a Rússia e a Ucrânia usando como domínio a internet que prevalece em grande parte dentro do conflito, como por exemplo, o desenvolver paciente dos russos dentro da estrutura virtual ucraniana em diversos *backdoors* - pontos ou portas de acesso para explorar vulnerabilidades e permitir a tomada de controle por agentes ilícitos, ou até um tipo de ataque comum no conflito Rússia-Ucrânia como o uso de software do tipo *data wiper* (apagador de dados)(SUZUKI, 2022).

Ademais, a sabotagem ao programa nuclear do Irã nos centros nevrálgicos do programa atômico iraniano, sofreu por meio de um blecaute,

quando os computadores foram verificados com um potente vírus desenvolvido para sabotar as usinas de enriquecimento de urânio do Irã, em 2010, com um grande nível de avanço atribuído a Israel e os EUA.

Logo, além de ataques às redes do sistema, outros serviços públicos também podem virar alvos, como o mercado financeiro, os serviços de distribuição de água potável, as telecomunicações e o setor de segurança. Em 2009, a divisão chinesa do Google foi alvo de um ataque considerado de alta gravidade por invasão de e-mails dos usuários e acesso aos códigos internos dos serviços da empresa. Os responsáveis nunca foram identificados, mas acredita-se que os invasores estavam interessados em documentar as movimentações de adversários do regime chines (GARRETT, 2022)

5. A GUERRA CIBERNÉTICA EM FACE À SUA ESCASSEZ NORMATIVA

5.1 A necessidade de regulamentação da Ciberguerra

Frente à dissipação de conteúdos e, bem ainda, comprado à “digitalização” dos serviços públicos e privados computadorizados surge, tendo como ponto de partida os ciberataques sofridos contra a Estônia no ano de 2007, a necessidade de regulamentação para os conflitos cibernéticos (IRIS-BH, 2016).

Para isso, a partir de 2009, na capital da Estônia, Tallinn, um grupo de estudiosos e experts no Direito Internacional elaboram o "Manual de Tallinn" que, nas palavras do Instituto de Referência em Internet e Sociedade(IRIS-BH, 2016), atuam como:[...] um centro de excelência em ciberdefesa no âmbito da Organização do Tratado do Atlântico Norte (OTAN), assim surge o Centro de Excelência em Ciberdefesa Cooperativa, que tem status de organização militar internacional.

Nas palavras de Michael Schmitt (2013, *apud* VITORINO, 2021):

> [...] o Manual de Tallinn identifica o direito internacional aplicável à guerra cibernética e estabelece noventa e cinco "regras sólidas" que regem esses conflitos. Aborda tópicos como soberania, responsabilidade do Estado, o jus ad bellum, Direito Internacional Humanitário e Direito da Neutralidade. Um extenso comentário acompanha cada regra, que estabelece a base de cada regra no tratado e na lei consuetudinária, explica como o Grupo de Especialistas interpretou as normas

> aplicáveis no contexto cibernético e descreve quaisquer divergências dentro do grupo quanto à aplicação de cada regra.

Desta feita, o ”Manual de Tallinn", elaborado por especialistas na área de ciberconflitos, pode ser compreendido como:

> [...] um documento acadêmico não vinculativo, que disserta sobre a interpretação da lei internacional com o objetivo de encontrar discernimento mais claro em casos legais complexos que envolvam ciberguerras e ciberoperações, com particular atenção às linhas de pensamento do direito humanitário *jus ad bellum* e *jus in bello* (IRIS-BH, 2016).

Dispõe da mesma forma o art. 2º da Carta das Nações Unidas, disciplinando a respeito da proibição do uso da força, o qual somente se "justifica"quando autorizado pelo Conselho de Segurança das Nações Unidas, qual seja na hipótese de legítima defesa e desde que respeita a necessidade e proporcionalidade dos ataques. Desta feita, se faz importante destacar, exemplificativamente, série de requisitos necessário para essa utilização dessa força segundo o "Manual de Tallinn" (IRIS-BH, 2016):

> a) Severity: qualquer operação cibernética que resulte em dano, destruição, ferimentos e mortes será considerada uso da força;
> b) Immediacy: quanto mais rápido se manifesta os efeitos de um ataque, menos meios um estado tem para se defender e, portanto, mais severos são seus danos;
> c) Directness: o nexo causal de um ataque cibernético;
> d) Invasiveness: um ataque cibernético que derrube ou invada o sistema militar, ou um sistema bem protegido de um Estado, será considerado mais intrusivo e, portanto, mais agressivo do que um ataque que derrube um sistema de serviços online com poucos defesas, como os de uma loja virtual de um cidadão comum;
> e) Measurability of Effects: o valor quantitativo dos danos causados, como o número de servidores derrubados, dados corrompidos, arquivos confidenciais roubados, etc.;
> f) Military Character: o nexo do uso de forças militares relacionados a um ataque;
> g) State Involvement: a extensão e o envolvimento contínuo sobre operações cibernéticas conduzidas por um Estado;
> h) Presumptive Legality: presunção legal sobre normas e tratados internacionais.

Desta feita, compreende-se que o "Manual de Tallinn" e a Carta da Nações Unidas atuaram, a partir de normas internacionais interativas já aceitas e aplicadas pela maioria dos Estados fora do espaço cibernético, como uma

série de “critérios” exemplificativos para entender os efeitos e a prática do uso de força armada (IRIS-BH, 2016) servindo, inclusive, como pressuposto para os indícios de regulamentação dessa nova modalidade de guerra assimétrica.

5.2 A intervenção do Conselho de Segurança das Nações Unidas para regulamentação da Guerra Cibernética frente à necessidade de criação de Tratados Internacionais

Diante da necessidade da criação de tratados internacionais referentes à regulamentação da Guerra Cibernética, é inegável que a interposição do Conselho de Segurança das Nações Unidas se faz necessária. Porém, como expandido ao decorrer deste tópico, o histórico de tentativas para a regulamentação do ciberespaço não é recente na ONU (BASU, 2021).

Em 1999, a Rússia propôs um projeto abrangendo "princípios da segurança internacional da informação", este, entretanto, teve pouco acolhimento pela Secretaria-Geral da ONU (CIGLIC, 2021).

Já em 2004, a ONU estabeleceu um Grupo de Peritos Governamentais ("Group of Governmental Experts" - GGE) das Nações Unidas sobre segurança cibernética, a fim de desenvolver normas de comportamento responsável dos Estados no ciberespaço no contexto de segurança internacional. Desde sua criação, seis GGEs foram estabelecidas até o presente ano, algumas com avanços essenciais para o processo de regulamentação no ciberespaço (CIGLIC, 2021).

O Grupo de Peritos Governamentais de 2013 teve um desenvolvimento notável para a época por delinear o primeiro conjunto de normas cibernéticas, bem como reafirmou que o Direito Internacional, a soberania dos Estados e os Direitos Humanos se aplicam ao ciberespaço (CIGLIC, 2021).

Mais adiante, no relatório do GGE de 2015, foi elaborado o princípio da não intervenção nos assuntos internos de outros Estados, salientando que os mesmos devem proteger as suas próprias infraestruturas cruciais (incluindo saúde, rede elétrica, educação, serviços financeiros, transporte, telecomunicações e processos eleitorais) e, de igual natureza, devem privar-se de realizar ataques cibernéticos que danifiquem infraestruturas cruciais de outros Estados. A existência de um rol taxativo de setores específicos que

devem ser reconhecidos como "infraestruturas críticas", também estabelecido nesse relatório, ajuda como um direcionamento de investimentos em segurança, como também devem ser vistos como uma linha vermelha para comportamentos maliciosos de Estados que - quando ultrapassados - geram consequências (CIGLIC, 2021).

Enfim, a última iniciativa até o presente momento na tentativa de conceber regras para o comportamento responsável dos Estados no ciberespaço, como uma forma de manutenção da paz e de segurança internacional foi o Grupo de Trabalho Aberto das Nações Unidas (“OEWG” - Open Ended Working Group) sobre Tecnologias de Informação e Comunicação, promovido por uma Resolução da Rússia, cujos relatórios não fizeram aditamentos concretos e escaparam das questões-chave, não cumprindo com os principais objetivos do OEWG, de abordar as causas profundas da instabilidade cibernética global nos dias de hoje (BASU, 2021).

Diante de todo o atraso dos Estados para o estabelecimento de regras no âmbito cibernético, a sofisticação das figuras ameaçadoras não parou de avançar. Consequentemente, o sistema internacional permanece vulnerável pela falta de responsabilização e por garantias insuficientes para civis e para as infra estruturas críticas dos Estados, levando à imprevisibilidade, à insegurança jurídica e à falta de responsabilização dos envolvidos (CIGLIC, 2021).

CONSIDERAÇÕES FINAIS

O âmbito jurídico tem testemunhado o surgimento de diversos fenômenos cibernéticos, haja vista, o crescimento exacerbado quanto a incidência de diferentes crimes virtuais, e ainda, recentemente é fato que vários indivíduos estão agindo sob a tutela do anonimato, o que confirma a existência de uma Guerra Cibernética desregularizada em curso.

As constantes sabotagens à programas de governo que, como serviços essenciais, lesionam as regras contidas no Direito Humanitário de Guerra com ações desequilibradas que não são de caráter legítimo com ataques dirigidos indiretamente contra civis, sem a mínima proporcionalidade e a precaução sem evitar qualquer dano aos civis, assim, comprovando que o espaço cibernético como algo de domínio amplo.

Esta nova modalidade de conflito traz ações ofensivas, defensivas e/ou exploratórias, realizadas no espaço cibernético. Diante disso, observam-se crises geopolíticas e sociais ligadas a esse avanço tecnológico, uma vez que o direito não consegue acompanhar as inseguranças individuais dos usuários, agredindo silenciosamente e de maneira inevitável os direitos humanos pelo avanço da mídia e seus perfis que desintegram o sigilo das informações, existentes em computadores, redes e sistemas de informação, em proveito próprio, tanto na área militar quanto na área civil.

Ademais, é constatado que o CIGE (Centro de Instrução de Guerra eletrônica), órgão gestor e formador dos recursos humanos para atuação cibernética, formou uma turma de militares ainda em 2012 (BOMBASSARO, 2018). De maneira que, tal formação de combate no espaço cibernético, é recente e tem efeito de pequena incidência, mesmo com o sistema se preparando para a defesa contra ações de exploração, ainda deixa a desejar quando há ações de ataque e defesa cibernéticas.

Os estudiosos do Direito Internacional, como o Instituto Iris-BH (2016), apresentem interpretações não vinculadas sobre os complexos no espaço cibernético expressando normas alinhadas ao direito humanitário que poderiam compor as norma da guerra na pauta internacional. Entretanto, o Estado ainda está em constante atraso para o estabelecimento das regras ao universo cibernético que comporta figuras ameaçadoras que não vão parar de avançar se continuarem sem delimitação.

A falta de controle que acompanha a superfluidez da informação no espaço cibernético, como máquina, não pode ser comparada às limitações do ser humano, como indivíduo oprimido,pelas dimensões da hipercodificação ligadas a Guerra Cibernética, sem meios favoráveis ao ambiente civil e jurídico, deixando o sistema internacional e nacional vulnerável pela falta de responsabilização e por garantias insuficientes para civis e para as estruturas governamentais de cada nação, levando à imprevisibilidade, e a mais atual insegurança jurídica.

REFERÊNCIAS

BASU, Arindrajit et al. **The UN Strugglesto Make ProgressonSecuring Cyberspace**. Carnegie Endowment for International Peace, 2021. Disponível em: https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491. Acesso em 20 de dez. de 2022.

BOBBIO, Norberto.**A Era dos Direitos**. Trad. Calos Nelson Coutinho.10 Ed. Rio de Janeiro: Campus, 1992.

BOMBASSARO NETO, Samuel. **A atuação da Guerra Cibernética como elemento multiplicador do poder de combate da Força Terrestre Componente em operações ofensivas.** 2018. 55 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/3913/1/MO%206013%20-%20BOMBASSARO.pdf. Acesso em: 21 de nov. de 2022.

BRASIL, Exército. Estado-Maior. **Guerra Cibernética.** Brasília, DF. 2017.

BRASIL, Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.**Brasília, DF. 2014.

CAMPOS NETO, Carlos W. M. O Princípio da Ordem Pública e a Cooperação Jurídica Internacional. **Prisma Jurídico [Online]**. 2014; v. 13 n. 2, p. 41-51. Disponível em: https://www.redalyc.org/articulo.oa?id=93443252004. Acesso em 13 de nov. de 2022.

CASTELLS, M. **A Sociedade em rede**. Tradução de Roneide Venancio Majer, vol. 1, 6 ed., São Paulo: Paz e Terra, 1999.

CIBERNÉTICA. In: DICIO, Dicionário Online de Português. Disponível em: https://www.dicio.com.br/cibernetica/. Acesso em 01 mar. 2023.

CIBERNÉTICA. **Portal São Francisco**. Disponível em: https://www.portalsaofrancisco.com.br/biologia/cibernetica. Acesso em 01 nov. 2022.

CHAVES, Viviane Hengler Corrêa. **A Revolução Cibernética:** A nova cultura. 2010. Disponível em: https://www.ufjf.br/ebrapem2015/files/2015/10/gd5_viviane_chaves1.pdf. Acesso em 01 nov. 2022.

CIGLIC, Kaja. O próximo capítulo da diplomacia cibernética nas Nações Unidas. **Microsoft News**, 2021. Disponível em: https://news.microsoft.com/pt-br/o-proximo-capitulo-da-diplomacia-cibernetica-nas-nacoes-unidas/.Acesso em 20 de dez. de 2022.

CLAUSEWITZ, Carl Von. **Da Guerra**. Tradução de Maria Teresa Ramos, 2 ed., São Paulo: Martins Fontes, 2003.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **CICV: Comitê Internacional da Cruz Vermelha**. A Guerra e o Direito. Disponível em: https://www.icrc.org/pt/guerra-e-o-direito. Acesso em 11 de set. 2022.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **CICV: Comitê Internacional da Cruz Vermelha.** O que é o direito internacional humanitário? Disponível em: https://www.icrc.org/pt/doc/resources/documents/misc/5tndf7.htm#:~:text=O%20Direito%20Internacional%20Humanit%C3%A1rio%20pro%C3%ADbe,ou%20duradouros%20ao%20meio%20ambiente. Acesso em 07 de set. 2022.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. **CICV: Comitê Internacional da Cruz Vermelha.** Regras básicas do Direito Humanitário Internacional nos conflitos armados. Disponível em: https://www.icrc.org/pt/doc/resources/documents/misc/basic-rules-ihl-311288.htm. Acesso em 07 de set. 2022.

DOLINGER, Jacob. **Direito Internacional Privado**: do Princípio da Proximidade ao Futuro da Humanidade. Direito & Amor. Rio de Janeiro: Renovar, 2021.

FERREIRA, Aurélio Buarque de Holanda. **Míni Aurélio:** O dicionário da língua portuguesa.

FERREIRA, Lívia. A Revolução das tecnologias de informação e comunicação: consequências sociais, econômicas e culturais. **Revista Digital de Biblioteconomia & Ciência da Informação**, n. 2, v. 7, p. 117-127, 2009. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/1978/2099. Acesso em 01 nov. 2022.

GARRETT, Filipe. O que é guerra cibernética? Entenda como funcionam os ataques virtuais.**Techtudo Segurança.** Disponível em: https://www.techtudo.com.br/noticias/2022/03/o-que-e-guerra-cibernetica-entenda-como-funcionam-os-ataques-virtuais.ghtml. Acesso em: 21 de nov. de 2022.

GUERRA. In: DICIO, Dicionário Online de Português. Disponível em: https://www.dicio.com.br/guerra/. Acesso em 01 mar. 2023.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE – BELO HORIZONTE (IRIS-BH). Manual de Tallinn e po uso da força. **IRIS - Instituto de Referência em Internet e Sociedade**. Disponível em: https://irisbh.com.br/manual-de-tallinn-e-o-uso-da-forca/. Acesso em: 14 de jan. de 2023.

INTERNATIONAL COMMITTEE OF THE RED CROSS. **ICRC: InternationalCommitteeof The Red Cross.** IHL andhumanrightslaw. Disponível em: https://www.icrc.org/en/doc/war-and-law/ihl-other-legal-

regmies/ihl-human-rights/overview-ihl-and-human-rights.htm. Acesso em 07 de set. de 2022.
INTERNATIONAL COMMITTEE OF THE RED CROSS. **ICRC: InternationalCommitteeof The Red Cross.**Treatiesandcustomarylaw. Disponível em: https://www.icrc.org/en/document/treaties-and-customary-law. Acesso em 07 de set. de 2022.

JOBIM, Amandha. O que é Direito Internacional Humanitário? **IHL Clinic UFRGS**. Porto Alegre, jun. 2021. Disponível em: https://www.ufrgs.br/ihlclinic/o-que-e-direito-internacional-humanitario/. Acesso em 11 de set. 2022.

MOORE, R. BeyondOurControl? Confrontingthe Limits ofOur Legal System in the Age of Cyberspace. **International Social Science Review**, [s. l.], v. 79, n. 3/4, p. 161–162, 2004. Disponível em: https://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=15558980&lang=pt-br&site=ehost-live. Acesso em: 20 dez. 2022.

MAZZUOLI, Valerio de O. **Curso de Direito Internacional Público**. Rio de Janeiro: Grupo GEN, 2021. Disponível em:https://integrada.minhabiblioteca.com.br/reader/books/9786559641307/epubcfi/6/74[%3Bvnd.vst.idref%3Dpt06chapter02]!/4. Acesso em 14 jan. 2023.

NARDO, Catelan Giovanna. O Direito Humanitário e os limites da Guerra. **Politize!** Florianópolis, jun. 2017. Disponível em: https://www.politize.com.br/direito-humanitario-limites-da-guerra/. Acesso em 11 de set. 2022.

PINHEIRO, Patrícia Peck. **Cyber Rights: Direitos Fundamentais dos cidadãos digitais e a existência de uma Ordem Pública global através da Internet**. REVISTA DOS TRIBUNAIS. São Paulo: Revista dos Tribunais, v. 105, n. 971, p. 624, set. 2016.

PIOVESAN, Flávia. **Direitos Humanos e o Direito Internacional Constitucional**. 19 Edição. São Paulo: Saraiva Educação, 2021.

SARLET, Ingo; SARLET, Gabrielle; BITTAR, Eduardo. **Inteligência Artificial, proteção de dados pessoais e responsabilidade na era digital**. São Paulo: Saraiva Educação, 2022.

SASSÓLI, Marco**. International Humanitarian Law:** Rules, Controversies, and Solutions to Problems Arising in Warfare. 101. ed. Cheltenham: Edward Elgar Pub, 2019. p. 951-958.

SOARES, Filipe Rocha Martins; RIBEIRO, Gustavo Ferreira. **Conflitos entre ordens públicas no espaço cibernético: uma abordagem cosmopolita em resposta à sobreposição regulatória da internet**. Revista de informação legislativa: RIL, v. 54, n. 216, p. 45-66, out./dez. 2017. Disponível em: https://www12.senado.leg.br/ril/edicoes/54/216/ril_v54_n216_p45. Acesso em 13 de nov. de 2022.

SUZUKI, Shin. A guerra cibernética paralela entre Rússia e Ucrânia. **BBC News Brazil,** São Paulo, 01 de março de 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60551648. Acesso em: 21 de novembro de 2022.
SWINARSKI, Christophe. **Direito internacional humanitário como sistema de proteção internacional da pessoa humana:** principais noções e institutos. São Paulo: Revista dos Tribunais, 1996.

VITORINO, L. G. **Direito Internacional e Ciberguerra:** Ataques Cibernéticos entre Nações, Manual de Tallinn, porque é mais fácil regular uma Ciberguerra do que regular uma Cibersegurança?. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas. Goiàs, 2021. Disponível em: https://repositorio.bc.ufg.br/bitstream/ri/19795/2/TCCG%20-%20Direito%20-%20Lu%C3%A3%20Gon%C3%A7alves%20Vitorino%20-%202021.pdf. Acesso em 14 jan. 2023.