**O DIREITO INTERNACIONAL HUMANITÁRIO E O CRIME DE GUERRA NA ERA DIGITAL: APLICA-SE O JUS IN BELLO NO CIBERESPAÇO?**

Os conflitos internacionais ganham novos contornos ao longo do tempo, novas possibilidades, áreas, espaços e armas. Nesse sentido, a internet – tal como outros avanços tecnológicos do passado – representa, ao mesmo tempo, um instrumental de desenvolvimento e aproximação, mas também de ataques e vulnerabilidades notórias (NUNES, 2015). A tecnologia à serviço da guerra é uma constante na história da humanidade. Momentos de guerra representam um forte impulso de inovação, principalmente nos setores militares. Isso leva ao incremento do estado da arte ou mesmo na criação de novas tecnologias – a exemplo dos computadores, dos aviões, motores automobilísticos e mesmo da própria internet – que mais tarde servem também a fins pacíficos). De fato, foi a Guerra Fria que intensificou o uso da tecnologia como representação de poder em um mundo em conflito. Essas eventualidades associam a guerra à tecnologia e devem ser enxergadas como de necessária compreensão temporal na era da globalização (FERNANDES, 2019), haja vista que as relações entre os Estados no tecido internacional cada vez mais são cruzadas no ciberespaço. Conforme Mazzuoli (2019, p.1660), a definição de guerra deve se pautar estritamente em termos jurídicos, sendo considerada “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)”. Não obstante, após a situação devastadora provocada pelos conflitos bélicos no século XX, a comunidade internacional passou a tratar a guerra como um ato de violência inadmitido no Direito Internacional, ou seja, internacionalmente ilícito (MAZZUOLI, 2019). Tais atos passaram a ensejar responsabilidade na esfera externa perante o Tribunal Penal Internacional, uma vez que o Estatuto de Roma prevê em seu art. 8º um rol de condutas que configuram o crime de guerra, estas que vão desde humilhações e ultrajes à dignidade da pessoa até o descumprimento das Convenções de Genebra de 1949 (ESTATUTO DE ROMA, 1998). Ademais, ao encontro do exposto, também houve na esfera internacional, a reivindicação de que os conflitos se tornassem menos desumanos e violentos, confeccionando-se instrumentos como tratados que aproximaram a guerra à uma humanidade por intermédio dos conceitos de *jus ad bellum* (o direito da guerra, ou seja, o direito ao uso da força), e o *jus in bello* (o direito na guerra, que visa regulamentar a maneira como a guerra é conduzida), percebidos tanto no próprio Estatuto de Roma como nos protocolos adicionais à Convenção de Genebra, consolidando então o chamado Direito Internacional Humanitário (DIH), que tem por objetivo limitar os efeitos da guerra ao proteger os que dela não fazem parte e restringir os meios e métodos aplicados por ela (CICV, 2010). Saindo dessa concepção clássica da guerra, é sabido que hodiernamente os conflitos na comunidade internacional passaram a enfrentar outro desafio: a internet e todos os desdobramentos inerentes à era digital, haja vista que a utilização da rede mundial de computadores torna a sociedade cada vez mais dependente desse mundo *on-line*, fato esse que traz consigo a ameaça inexorável de um ataque cibernético. Portanto, essa vulnerabilidade é observada por determinados grupos como uma oportunidade, onde “o mundo passa a conviver com a sombra do ciberterrorismo e, no caso dos Estados, com a possibilidade de hostilidades no ciberespaço, ou seja, uma Guerra Cibernética” (NUNES, 2010 p.11). A guerra cibernética surge então como um novo episódio belicoso, decorrente da inevitável transformação e adequação dos conflitos à era digital (SILVA E SILVA, 2019), o seu conceito vincula-se à massiva participação dos Estados no meio digital concomitantemente à presença de atores não estatais, tais como grupos terroristas, por exemplo, porém é preciso deixar claro que o Direito Internacional Humanitário por sua natureza não se aplica a casos de cibercriminalidade ou ciberterrorismo (MELZER, 2011). Entretanto, em uma definição precisa, considera-se guerra cibernética o conflito travado por dois ou mais estados no ciberespaço (NUNES, 2010), em que há a invasão de computadores ou redes de outra nação com o objetivo de causar transtornos, obter informações, corromper dados, entre outros danos que podem ser irreversíveis (CLARKE; KNAKE, 2015). Por sua vez, o ciberespaço pode ser aqui descrito como uma “rede globalmente interconectada de informações digitais e infraestruturas de comunicações, incluindo a Internet, redes de telecomunicações, sistemas informáticos e as informações neles residentes” (MELZER, 2015 p.4). Destarte, infere-se que a utilização da internet e de suas ferramentas para efetivar as práticas violadoras pode inclusive ser observada nessa situação como equiparadas a utilização de armamento previsto no conceito clássico de guerra, uma vez que da mesma forma a internet é o meio instrumentalizador para alcançar-se o objetivo. Ante a todo o supracitado, entende-se necessário o questionamento: Nesse contexto de guerra cibernética, partindo de uma concepção no DIH, é possível a aplicação do *jus in bello* enquanto meio mitigador**?** E em casos de descumprimento é possível a responsabilização internacional do Estado comandatário perante o Tribunal Penal Internacional?. A hipótese é que mesmo não existindo uma referência específica acerca da guerra entre Estados no ciberespaço na Convenções de Genebra, o espaço cibernético configura-se como um novo domínio de guerra na era digital, não restando dúvidas que o Direito Internacional Humanitário é cabível nesse ambiente, pois as normas e princípios observados nos tratados que regulamentam os meios e métodos da guerra para impedir violações a direitos humanos e civis representam o momento histórico de sua criação mas não se prendem a ele, podendo haver a ampliação da aplicabilidade ante a evolução dos meios e ambientes de guerra. Diante dessa perspectiva, esse trabalho tem como objetivo geral demonstrar se ao crime de guerra cibernética também pode ser aplicado os meios que limitam a agressividade da guerra no seu sentido clássico, percebidos no âmbito do Direito Internacional Humanitário. Especificadamente pretende-se compreender em que termos o Estado comandante da guerra no ciberespaço pode ser responsabilizado internacionalmente perante o Tribunal Internacional Penal (TPI) por descumprimento às restrições supracitadas. Para tanto, a metodologia aplicada foi a qualitativa, utilizando-se do procedimento da bibliografia, onde analisando, refletindo acerca dos conceitos de guerra e ciberespaço pode-se chegar a iniciais debates sobre a convergência do crime de guerra cibernética junto o Direito Internacional Humanitário e sua responsabilização perante a Corte Internacional Penal. Assim, em uma discussão preambular, pode-se inferir que a segurança cibernética dos Estados passou a ser um ponto importantíssimo decorrente da crescente necessidade de utilização destes meios, e por conta disso, quando analisa-se as problemáticas que envolvem o ciberespaço e o crime de guerra percebe-se uma certa dificuldade na caracterização das atividades hostis e degradantes que ocorrem nesta conjuntura colocam em dúvida a aplicabilidade do Direito Internacional Humanitário (JASTRAM E QUINTIN, 2011). Todavia, sendo um fenômeno frequentemente estudado, nota-se que o DIH já previu antecipadamente as formas evolutivas no uso de armas e o aprimoramento ou desenvolvimento de meios e métodos novos para instrumentalizar a guerra, presumindo-se que o DIH é aplicável a eles (CICV, 2019). O art. 36 do Protocolo adicional I de 1977 à Convenção de Genebra disciplina o estudo, preparação, aquisição ou adoção de uma nova arma, isto é, de novos meios ou de um novo método de guerra, coisa que não o faz de forma específica, haja vista ao estabelecer-se que a alta parte contratante tem a obrigação de determinar se o emprego da nova arma seria proibido por alguma norma ou tratado de Direito Internacional, deixa-se um lacuna na norma, pois nem o DIH nem outro instrumento internacional disciplinou as proibições ou limitações no uso dos meios cibernéticos durante a guerra (SILVA E SILVA, 2019). Destarte, os princípios e normas humanitárias que mitigam a violência da guerra podem ser aplicáveis a um conflito cibernético atribuído a um Estado, mas somente por razão de algo que supere um eventual incidente, bem como possua o propósito de causar a danos, destruição, ferimentos e até mesmo a morte, ainda que as forças armadas não se manifestem em seu sentido clássico, isto é, presencialmente (SCHIMITT, 2012). Outrossim, para o Comitê Internacional da Cruz Vermelha (CICV, 2019) é indubitável a noção de que o DIH limita também as operações cibernéticas durante conflito armado, fala-se, inclusive, que esse fato se atrela de forma fundamental na Opinião Consultiva do Corte Internacional de Justiça (CIJ) acerca da legalidade da ameaça ou uso de armas nucleares, onde o tribunal lembrou que os princípios e regras do DIH são conferidos às diversas formas de guerra e a todos as espécies de armas, as quais se incluem as “armas do futuro”, como a Internet (CIJ, 1996). Nesse sentido, conclui-se que proteções que objetivam resguardas a comunidade civil frente às hostilidades do conflito armado, são também notadas no ciberespaço. Por exemplo, nos ataques cibernéticos, o princípio fundamental da distinção (previsto no art. 48 do Protocolo adicional I de 1977 à Convenção de Genebra) é imprescindível para evitar atentados indiscriminados, visto que os beligerantes devem distinguir em todos os momentos a população civil e combatentes, bem como diferenciar os objetos civis e objetivos militares, e encaminhar suas operações apenas contra os objetivos militares. Além disso, é sabido que no que toca à responsabilização do ator comandante da guerra no ciberespaço nota-se que o ambiente digital fornece outro desafio, pois nesse espaço os beligerantes podem falsificar a identificação ou utilizar-se de meios que camuflam ou escondem totalmente a identificação dos ataques, o que dificulta a atribuição de guerra por outros atores internacionais, e isso acaba por refletir também na aplicação do *jus in bello*, pois o DIH somente se aplica às operações que se relacionem com o conflito (CICV, 2019). Essa noção de guerra em um espaço que há pouco tempo não era tão utilizado representa ao olhos do Direito Internacional e do Direito Humanitário um complexo que ainda requer em determinadas questões uma especialização jurídica internacional por meio de um tratado, que pode por intermédio do bom senso estabelecer medidas que resolvam omissões acerca da aplicação do DIH à guerra cibernética, isso porque esse é um campo em crescente constante e que quando não cooperado entre atores internacionais ocasiona sérios riscos aos direitos civis.

**Palavras-chave:** Guerra, Ciberespaço, Direito, Humanitário.

**Referências**:

CICV. Comitê Internacional da Cruz Vermelha. **O DIH e outros regimes legais – jus ad bellum e jus in bello**. 2010. Disponível em: https://www.icrc.org/pt/doc/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm. Acesso em: 06 nov. 2020.

CICV. Comitê Internacional da Cruz Vermelha**. Direito Internacional Humanitário e Operações Cibernéticas durante conflitos armados: Documento de posição do CICV**. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj7pse40-\_sAhWlKrkGHYVxBiQQFjABegQIARAC&url=https%3A%2F%2Fwww.icrc.org%2Fen%2Fdownload%2Ffile%2F108983%2Ficrc\_ihl-and-cyber-operations-during-armed-conflicts.pdf&usg=AOvVaw2kNTiTQIOQrzd1\_iAle1I9. Acesso em: 06 nov. 2020.

FERNANDES, José Pedro Teixeira. **Geopolítica em Tempo de paz e Guerra**. 1 ed. São Paulo: Almedina, 2019.

JASTRAM, Kate; QUINTIN, Anne. The internet in bello: cyber war law, ethics & policy. In: CYBERWARFARE SEMINAR, 2011, Berkeley. **Proceedings…** Berkeley, 2011. Disponível em: https://www.law.berkeley.edu/files/cyberwarfare\_seminar-- summary\_032612.pdf. Acesso em: 6 nov. 2020.

KNAKE, Robert K.; CLARKE, Richard A. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015. 280 p.

MAZZUOLI, Valerio de Oliveira. **Curso de Direito Internacional Público**. 12. ed. Rio de Janeiro: Forense, 2019. 1797 p.

MELZER, N. **Cyberwarfare and international law**. Genebra, Suiça: United Nations Institute for Disarmament Research, 2011. Disponível em: http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Acesso em: 6 nov. 2020.

NUNES, Luiz Artur Rodrigues. **GUERRA CIBERNÉTICA E O DIREITO INTERNACIONAL: Aplicabilidade do Jus ad Bellum e do Jus in Bello**. 2015. 60 f. TCC (Graduação) - Curso de Altos Estudos de Política e Estratégia, Escola Superior de Guerra, Rio de Janeiro, 2015. Disponível em: https://egov.ufsc.br/portal/conteudo/guerra-cibern%C3%A9tica-e-o-direito-internacional-aplicabilidade-do-jus-ad-bellum-e-do-jus-bello. Acesso em: 05 nov. 2020.

NUNES, Luiz Artur Rodrigues. **GUERRA CIBERNÉTICA: Está a MB preparada para enfrenta-la?.** 2020. 99 f. TCC (Graduação) - Curso de Política e Estratégia Marítimas., Escola de Guerra Naval, Rio de Janeiro, 2010. Disponível em: http://www.redebim.dphdm.mar.mil.br/vinculos/000006/000006d7.pdf. Acesso em: 06 nov. 2020.

SCHMITT, Michael N. Wired warfare: computer network attack and jus in bello. **International Review of the Red Cross**, Suíça, v. 84, n. 846, p. 365-399, June, 2012. Disponível em: https://www.icrc.org/en/doc/assets/files/other/365\_400\_schmitt.pdf. Acesso em: 6 nov. 2020.

SILVA, Rodrigo Cardoso; SILVA, Eliza Odila Conceição. O dilema do Jus ad Bellum e Jus in Bellum na Guerra Cibernética: como aplicar o direito da guerra na era digital? In: JUBILUT, Liliana Lyra et al (org.). **Direitos Humanos e Vulnerabilidade e o Direito Humanitário**. Boa Vista: Editora da UFRR, 2019. Cap. 1. p. 125-150. Disponível em: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiF66-J0O\_sAhXCJ7kGHTp1B3kQFjAAegQIAxAC&url=https%3A%2F%2Fufrr.br%2Feditora%2Findex.php%2Feditais%3Fdownload%3D421&usg=AOvVaw1IW2TBs3r3S0KVMAvnmm8f. Acesso em: 06 nov. 2020.