REGULAMENTAÇÃO E RESPONSABILIDADES NA GUERRA CIBERNÉTICA

*Cap **Luiz Paulo** Lopes dos Santos*

RESUMO

Este artigo trata do comportamento do computador e seus efeitos sob uma perspectiva ética. O trabalho mostrará teorias, definições e limitações, considerando as teorias de autores como Singer, Friedman, Wittes, Blum, Ventre e Buchanan. Destaca a necessidade de coordenar e definir responsabilidades, tendo em conta as regulamentações existentes na Europa e nos Estados Unidos. Discute a ética e o bom senso na guerra cibernética e reconhece a dificuldade de estabelecer fronteiras. No contexto brasileiro, destaca diferenças na legislação e faz comparações com leis estrangeiras. Conclui destacando a importância de abordar questões éticas para garantir a segurança, a privacidade e a integridade na sociedade face aos desafios emergentes de segurança cibernética.

Palavras-chave: Cibernética, Responsabilidades, Legislação.

1. INTRODUÇÃO

O aumento da conectividade no mundo e a dependência da tecnologia, deram origem a um novo tipo de guerra: a guerra cibernética. Neste contexto, as ações cibernéticas tiveram um impacto significativo na segurança pública e internacional. A crescente complexidade destas práticas e as crescentes implicações da ética tornam cada vez mais importante impor regras e responsabilidades. Este trabalho aborda a questão das ações cibernéticas e suas consequências a partir de uma perspectiva ética. É necessária uma compreensão dos conceitos básicos do comportamento cibernético para avaliar as implicações éticas e as responsabilidades a eles associadas. Autores populares como Singer, Friedman, Wittes, Blum, Ventre e Buchanan contribuíram com teorias e estudos que lançam luz sobre questões éticas e a necessidade de definir limites nessas práticas.

Além disso, uma comparação das leis existentes em diferentes jurisdições, como os Estados Unidos e outros países europeus, revela diferentes abordagens à regulação do comportamento cibernético. O ambiente jurídico é influenciado pela ética, pela cultura e pela política e reflete a complexidade inerente à definição de responsabilidades num contexto global.

Contudo, a discussão sobre a ética e os limites da guerra cibernética é complicada pela natureza única do ambiente digital. Definir o que é aceitável e responsável no comportamento cibernético exige um equilíbrio cuidadoso entre os objetivos de segurança e a preservação dos direitos humanos. A falta de limites físicos e a capacidade de trabalhar remotamente tornam ainda mais difícil identificar os responsáveis e manter os padrões morais.

Deste modo, explorar a dimensão ética do comportamento cibernético e as suas implicações sociais é essencial para encorajar uma discussão significativa sobre regras e responsabilidades. Os argumentos e perspectivas dos autores contribuem para a compreensão dos desafios de avaliar um ambiente cibernético seguro e ético.

2. DESENVOLVIMENTO

Segundo o livro "Cybersecurity and Cyberwar: What Everyone Needs to Know", Singer e Friedman (2014) argumentam que a cibersegurança é uma das questões mais urgentes da atualidade. Os autores destacam que as vulnerabilidades dos sistemas de computadores, combinadas com a crescente sofisticação dos hackers e das ameaças cibernéticas, tornam o mundo digital um lugar cada vez mais perigoso. Enfatizam a importância da cooperação internacional para enfrentar as ameaças cibernéticas. Segundo eles, é necessário estabelecer uma estrutura de governança global para a segurança cibernética, que inclua a definição de responsabilidades e limites nas ações cibernéticas. Os autores citam que a falta de regulamentação e responsabilidade pode levar a conflitos internacionais e instabilidade política e econômica.

Outros autores que corroboram, dando sua perspectiva em "The Future of Violence: Robots and Germs, Hackers and Drones - Confronting A New Age of Threat" de Wittes e Blum (2015), destacam a importância da definição de responsabilidades e limites nas ações cibernéticas para lidar com as ameaças cibernéticas. Os autores observam

que a falta de regulamentação e responsabilidade pode levar a uma série de problemas, como a escalada de conflitos internacionais, a disseminação de malware e a perda de privacidade e segurança para os usuários da Internet.

Argumentam que a regulamentação das atividades cibernéticas deve ser baseada em princípios claros e transparentes, que estabeleçam responsabilidades e limites para todos os atores envolvidos. Os autores enfatizam que a definição desses princípios deve ser baseada em um diálogo internacional, envolvendo governos, empresas, organizações da sociedade civil e usuários da Internet.

A importância da segurança cibernética para a defesa nacional e a estabilidade internacional, bem como a falta de regulamentação e responsabilidade nas atividades cibernéticas pode levar a conflitos internacionais, instabilidade política e econômica e ameaças à privacidade e segurança dos indivíduos, como cita outro autor Ventre (2012) em The Ethics of Cyber Conflicts. Routledge. Na abordagem deste trabalho, identificamos uma grande variedade de conceitos e definições relacionados à cibersegurança e às responsabilidades nas ações cibernéticas. Segundo Singer e Friedman (2014), a cibersegurança pode ser definida como o conjunto de medidas que visam proteger sistemas, redes e informações contra-ataques cibernéticos. Por outro lado, Wittes e Blum (2015) propõem uma definição mais ampla de cibersegurança, que inclui não apenas a proteção contra-ataques, mas também a garantia da privacidade, a proteção da propriedade intelectual e a manutenção da estabilidade dos sistemas e redes.

No que diz respeito às responsabilidades nas ações cibernéticas, Ventre (2012) destaca que é importante distinguir entre as responsabilidades de diferentes atores, como governos, empresas e usuários individuais. Segundo este autor, cada um desses atores tem um papel fundamental na garantia da cibersegurança e na prevenção de ataques cibernéticos.

Buchanan (2016), acrescenta que a definição de responsabilidades nas ações cibernéticas também deve levar em consideração a complexidade e a interdependência dos sistemas e redes, o que pode tornar difícil atribuir responsabilidades individuais em caso de ataques cibernéticos.

Por fim, Clarke e Knake (2010) enfatizam a importância da cooperação internacional para garantir a segurança cibernética e a definição de responsabilidades nas ações cibernéticas. Segundo os autores, a cooperação entre governos, empresas e usuários é essencial para enfrentar os desafios da cibersegurança em um mundo cada vez mais conectado e interdependente.

Neste contexto, foi possível observar que todos os autores geralmente concordam sobre definição única sobre a importância da definição das normas e acordos que regulem o comportamento dos estados e das empresas no espaço cibernético. Além disso, a proteção dos direitos fundamentais dos indivíduos, especialmente no que se refere à privacidade e à liberdade de expressão, é vista como um elemento chave na elaboração de políticas de cibersegurança eficazes.

Também foi destacado por todos os autores, a importância da colaboração internacional na definição de responsabilidades e limites nas ações cibernéticas. Como destacado por Singer e Friedman (2014), a cibersegurança é um problema global que requer esforços coordenados entre governos e organizações internacionais para garantir a segurança das informações em todo o mundo.

Da análise de todos os autores percebe-se que há uma necessidade urgente de se definir responsabilidades e limites nas ações cibernéticas, especialmente devido ao crescente número de ataques cibernéticos em todo o mundo. Os autores apresentados mostram abordagens e teorias diferentes sobre o tema, mas em geral concordam que é preciso uma abordagem mais colaborativa entre os setores público e privado, assim como este, sugere a necessidade de investimentos em tecnologias e políticas de segurança cibernética.

Ainda há muitas questões em aberto e desafios a serem superados, como a complexidade do cenário cibernético global, a falta de consenso internacional sobre o que constitui um ataque cibernético, e a dificuldade de atribuir responsabilidades em caso de ataque.

No entanto, identificamos algumas iniciativas positivas em curso, como a criação de organizações internacionais para tratar de questões de segurança cibernética, a elaboração de políticas nacionais e internacionais para combater a cibercriminalidade, e o desenvolvimento de tecnologias de defesa cibernética cada vez mais avançadas.

Os limites das ações cibernéticas são um tema complexo e controverso, e podem variar de

acordo com o contexto e a perspectiva de cada autor. No entanto, é possível apontar alguns limites que são amplamente defendidos na literatura e que podem ser vistos como éticos e realistas.

Do ponto de vista ético, é importante que as ações cibernéticas sejam realizadas com respeito aos direitos humanos, à privacidade e à proteção dos dados pessoais. Além disso, é fundamental que sejam evitados danos colaterais e que sejam adotadas medidas para minimizar os impactos negativos sobre terceiros.

Já do ponto de vista realista, é importante que as ações cibernéticas sejam realizadas de maneira proporcional e justificada, levando em conta os objetivos pretendidos e os riscos envolvidos. Isso significa que os governos devem evitar o uso indiscriminado de ferramentas cibernéticas e ações que possam gerar danos desproporcionais, seja em termos de custos econômicos ou de perda de vidas humanas.

Em geral, os limites das ações cibernéticas podem ser definidos por meio de uma combinação de políticas públicas, regulamentações, acordos internacionais e medidas técnicas de segurança. Essas medidas, se adotadas, terá de levar em conta de forma transparente e democrática as necessidades e os interesses dos diversos stakeholders envolvidos, como governos, empresas, organizações da sociedade civil e usuários finais.

As leis internacionais aplicáveis à guerra cibernética são complexas e estão em constante evolução. Em geral, as leis internacionais que regem a guerra cibernética se concentram em proibir o uso de força contra um Estado soberano sem autorização do Conselho de Segurança das Nações Unidas, além de estabelecer restrições ao uso de armas cibernéticas.

No Brasil, a regulamentação da guerra cibernética ainda está em desenvolvimento. Em 2017, foi criado o Comando de Defesa Cibernética (ComDCiber), que é responsável pela defesa cibernética do país e pela coordenação das atividades dos diversos órgãos governamentais envolvidos na segurança cibernética. Em 2021, o Ministério da Defesa divulgou a sua Política Nacional de Defesa Cibernética, que estabelece diretrizes para a defesa cibernética do país, incluindo a proteção de infraestruturas críticas e o desenvolvimento de capacidades de inteligência cibernética.

Além disso, o Brasil também tem se envolvido em discussões internacionais sobre a regulamentação da guerra cibernética. Em 2019, o país apoiou a criação do Grupo de Trabalho sobre a governança da segurança cibernética nas Nações Unidas e tem participado ativamente de discussões sobre o tema em outros fóruns internacionais.

No entanto, ainda há um longo caminho a percorrer para que a regulamentação da guerra cibernética esteja totalmente desenvolvida no Brasil e em todo o mundo. A complexidade do ambiente cibernético, juntamente com a natureza em constante evolução das ameaças cibernéticas, tornam difícil estabelecer um conjunto definitivo de regras para a guerra cibernética. É provável que essa seja uma área de debate contínuo no futuro próximo.

Atualmente no Brasil existem algumas leis que abordam o tema de ataques cibernéticos ou violação dos direitos cibernéticos, são elas: Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que trata da criminalização de condutas praticadas na internet, como invasão de dispositivos eletrônicos e divulgação de informações privadas. Também aprovada a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que estabelece regras para coleta, armazenamento e tratamento de dados pessoais, visando proteger a privacidade e os direitos dos titulares desses dados. Tem-se a Lei nº 14.155/2021, que dispõe sobre o combate ao crime cibernético e altera a Lei nº 12.735/2012 para incluir novos tipos penais relacionados à cibercriminalidade, como o furto de dados.

Além dessas, existem outras leis e normas que tratam de temas relacionados à cibersegurança, como a Lei nº 13.460/2017, que regula a participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública, e a Norma ABNT NBR ISO/IEC 27001:2013, que estabelece diretrizes para implementação de sistemas de gestão da segurança da informação.

Alguns exemplos de leis em outros países que definem responsabilidades sobre crimes cibernéticos e que poderiam ser aplicadas no Brasil são:

Estados Unidos: Computer Fraud and Abuse Act (CFAA) de 1986, que define os crimes cibernéticos e suas penalidades; Cybersecurity Information Sharing Act (CISA) de 2015, que incentiva a troca de informações entre empresas e governo para combater ameaças cibernéticas; e General Data Protection Regulation (GDPR) da União Europeia, que se aplica a empresas americanas que operam na UE.

Reino Unido: Computer Misuse Act de 1990, que criminaliza o acesso não autorizado a computadores e outras formas de interferência em sistemas de informação; e Data Protection Act de 2018, que implementa a General Data Protection Regulation (GDPR) da UE no Reino Unido.

Alemanha: Gesetz zur Verbesserung der IT-Sicherheit (IT-Sicherheitsgesetz) de 2015, que estabelece medidas de segurança cibernética para empresas de infraestrutura crítica; e Datenschutz--Grundverordnung (DSGVO) da UE, que se aplica a empresas alemãs que operam na UE.

França: Loi pour la Confiance dans l'Economie Numérique (LCEN) de 2004, que define crimes cibernéticos e responsabilidades para provedores de serviços da Internet; e RGPD (Règlement Général sur la Protection des Données) da União Européia, que se aplica a empresas francesas que operam na UE.

Essas leis podem servir de inspiração para a criação de uma legislação mais abrangente sobre crimes cibernéticos no Brasil.

Não existe uma bibliografia específica que estabeleça limites precisos e delimitações claras sobre o que pode ou não ser feito em um ataque cibernético. Na verdade, a questão dos limites éticos e legais da guerra cibernética ainda é um tema controverso e em constante evolução.

Algumas abordagens defendem a aplicação dos mesmos princípios éticos e legais da guerra convencional, enquanto outras argumentam que a natureza da guerra cibernética é tão diferente que exige uma abordagem totalmente nova. Por isso, os limites e responsabilidades em um ataque cibernético muitas vezes vão depender do bom senso, do contexto específico em que o ataque ocorre e da legislação aplicável em cada país.

Algumas das obras mencionadas anteriormente, como "Cyber War" de Richard Clarke e Robert Knake e "Cybersecurity and Cyberwar: What Everyone Needs to Know" de P.W. Singer, discutem essas questões de ética e limites em guerra cibernética, mas sem estabelecer limites precisos e delimitações claras.

3. CONCLUSÃO

Conclui-se que existe uma lacuna regulatória no Brasil, comparada com legislações dos Estados Unidos e Europa. Que o tema é complexo, do ponto de vista ético precisa-se enfatizar a necessidade de equilibrar segurança e direitos humanos.

Este artigo evidencia que definir limites e responsabilidades requer abordagem cautelosa, considerando o caráter dinâmico do ciberespaço. Assim, a análise dos argumentos e as lições extraídas são fundamentais para formar futuras regulamentações e estratégias, visando a construção de um ambiente cibernético seguro, ético e responsável.

Abstract

We will deal with computer behavior and its effects from an ethical perspective. The work will show theories, definitions and limitations, considering the theories of authors such as Singer, Friedman, Wittes, Blum, Ventre and Buchanan. It highlights the need to coordinate and define responsibilities, taking into account existing regulations in Europe and the United States. It discusses ethics and common sense in cyber warfare and recognizes the difficulty of establishing boundaries. In the Brazilian context, it highlights differences in legislation and makes comparisons with foreign laws. It concludes by highlighting the importance of addressing ethical issues to ensure security, privacy and integrity in society in the face of emerging cybersecurity challenges.

Keywords: *Cybernetics, Responsibilities, Legislation.*

4. REFERÊNCIAS

BUCHANAN, Ben. **The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations**. Ed. 1. Oxford University Press, 2016.

SINGER, P.W. e FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know**. Ed. 1. Illustrated, 2014.

WITES, Bejnamim e BLUM, Gabriella. **The Future of Violence: Robots and Germs, Hackers and Drones - Confronting A New Age of Threat**. Ed. 1. s/n: Blackstone Pub, 2015.