ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

ANÁLISE JURIMÉTRICA COMPARADA DA LEGISLAÇÃO ACERCA DE CIBERCRIME DO BRASIL E ESTADOS UNIDOS

COMPARATIVE JURIMETRIC ANALYSIS ABOUT THE BRAZILIAN AND AMERICAN CYBERCRIME'S LAW

RVD

Recebido em 05.04.2023
Aprovado em. 08.08.2023

Gabriel Soares Messias[1]

José Eronides de Sousa Pequeno Junior[2]

RESUMO
Um dos grandes desafios da conexão em massa é a regulação do ciberespaço, especialmente o controle da criminalidade na internet, que afeta dados em todas as nações. No Brasil, especificamente, no ano de 2017, 62,21 milhões de pessoas foram afetadas por crimes cibernéticos, resultando em um prejuízo de 22,5 bilhões de dólares. Assim, o Brasil ocupa o segundo lugar em danos financeiros causados por cibercrimes, ficando atrás apenas da China e seguido pelos Estados Unidos. O objetivo deste estudo é realizar uma análise comparativa entre o Brasil e os Estados Unidos a fim de compreender o estado da legislação em cada um desses países. Decidiu-se adotar o método hierárquico (nested) em conjunto com estatística descritiva, estudo de caso e análise qualitativa da legislação. As variáveis foram extraídas da Convenção de Budapeste, indicada por alguns autores como a legislação mais avançada sobre o tema. Considerando os resultados obtidos e a correspondência dos dados levantados com as variáveis, verificou-se que a legislação dos Estados Unidos e do Brasil possuem 90% de aderência aos parâmetros estabelecidos. Assim, pode-se concluir que não há disparidades expressivas entre a proteção conferida pelo ordenamento jurídico brasileiro e o estadunidense. No entanto, percebe-se que outros fatores podem estar envolvidos no fato de os danos financeiros sofridos pelos usuários brasileiros serem tão superiores.

PALAVRAS-CHAVE: Cibercrimes; Direito Comparado; Internet.

ABSTRACT
One of the great challenges of mass connectivity is the regulation of cyberspace, especially the control of internet crime, which affects data in all nations. In Brazil, specifically, in the year 2017, 62.21 million people were affected by cybercrime, resulting in a loss of 22.5 billion dollars. Thus, Brazil ranks second in financial damages caused by cybercrime, only behind China and followed by the United States. The objective of this study is to conduct a comparative analysis between Brazil and the United States in order to understand the state of legislation in each of these countries. It was decided to adopt the hierarchical (nested) method in conjunction with

[1] Pós-graduando em Direito Empresarial (EBRADI). Graduado em Direito (UNITINS). Email: gabrielsoaresmessias2020@gmail.com. ORCID: https://orcid.org/0000-0001-6947-2979
[2] Doutor em Ciência Política (UFPE). Professor do Curso de Direito da UNITINS – Campus Palmas. E-mail: eronides.sp@unitins.br

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

descriptive statistics, case studies, and qualitative analysis of legislation. The variables were extracted from the Budapest Convention, indicated by some authors as the most advanced legislation on the subject. Considering the obtained results and the correspondence of the collected data with the variables, it was found that the legislation of the United States has 90% compliance with the established parameters, while Brazil has 70%. Thus, it can be concluded that there are no significant disparities between the protection provided by the Brazilian legal system and the American one. However, it is perceived that other factors may be involved in the fact that the financial damages suffered by Brazilian users are so much higher.

KEYWORDS: Comparative Law; Cybercrime; Internet.

1 CONSIDERAÇÕES INICIAIS

A sociedade contemporânea é fortemente marcada pela conectividade, principalmente a partir da década de 1990, quando a internet se popularizou ao redor do globo. Atualmente, no Brasil, cerca de 71% da população possui acesso à rede (CETIC, 2019), tornando o ciberespaço um ambiente de múltiplas possibilidades que proporciona a interação de pessoas geograficamente distantes.

Neste cenário, surge um dos grandes desafios da conexão em massa: a regulação do ciberespaço, especialmente o controle da criminalidade na internet, que afeta dados em todas as nações. No Brasil, especificamente, no ano de 2017, 62,21 milhões de pessoas foram afetadas por crimes cibernéticos, resultando em um prejuízo de 22,5 bilhões de dólares (Symantec, 2017). Assim, o Brasil ocupa o segundo lugar em danos financeiros causados por cibercrimes, ficando atrás apenas da China e seguido pelos Estados Unidos.

Fazendo uma breve análise dos dados apresentados pela Symantec, nota-se que em 2017 a China registrou 352,70 milhões de pessoas que tiveram suas vidas afetadas por cibercrimes, enquanto suas perdas financeiras alcançaram 66,3 bilhões de dólares. Já os Estados Unidos registraram 143,70 milhões de pessoas afetadas e perdas de 19,8 bilhões de dólares no mesmo ano.

Esse panorama evidencia o quão significativamente maiores são as perdas brasileiras em comparação com as de outros países, como os Estados Unidos e a China, como proposto neste artigo. Vale ressaltar que a população brasileira é

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

consideravelmente menor do que a dessas nações mencionadas. Assim, o propósito deste artigo é mensurar o grau de proteção legal conferido pelo Brasil e pelos Estados Unidos no que diz respeito aos cibercrimes e analisá-los sob uma perspectiva comparativa.

Destaca-se que Presidente da República promulgou o Decreto nº 11.491, publicado no Diário Oficial da União em 12 de abril de 2023, para aceitar o convite do Conselho da Europa e aderir à Convenção sobre o Crime Cibernético firmada em Budapeste. Essa decisão fortalece os laços de cooperação com parceiros estratégicos no combate aos crimes cibernéticos, colocando o Brasil como um dos países que participam desse importante instrumento internacional.

De início, é fundamental apresentar o conceito de cibercrime. Segundo a OCED (Organização para a Cooperação e Desenvolvimento Econômico) da Organização das Nações Unidas, crimes de computador abrangem quaisquer comportamentos antijurídicos, não éticos ou não autorizados relacionados ao processamento ou transmissão de dados. Esses crimes ocorrem no meio informático e são considerados parte integrante do tipo legal, mesmo quando o bem protegido não é digital (Simas, 2014, p. 12).

Martin, citado por Lima (2011, p. 10), define crimes informáticos como ações dolosas que causam prejuízo a pessoas, utilizando dispositivos informáticos com esse propósito. Por sua vez, Costa (2011, p. 5) considera como crimes informáticos todas as ações típicas, jurídicas e culpáveis cometidas por meio do processamento automático de dados ou sua transmissão. A Interpol (2020), por sua vez, define cibercrime como atividade criminosa diretamente ligada a qualquer ação ou prática ilícita promovida pela internet.

Embora exista uma multiplicidade de definições sobre essa modalidade de crime, há um consenso geral em relação à natureza informatizada do cibercrime e à sua amplitude. Nem sempre as ações que causam danos aos usuários são tipificadas na legislação penal. Pode-se inferir que a dificuldade na definição do cibercrime reside na abrangência do fenômeno, o que apresenta desafios ao legislador devido à

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

variabilidade de condutas praticadas no mundo virtual, tornando sua adequada tipificação mais complexa.

2 METODOLOGIA

Este estudo optou por adotar o método hierárquico (*nested*), juntamente com estatística descritiva, estudo de caso e análise qualitativa da legislação.

O método hierárquico mostrou-se altamente adequado para a presente análise, uma vez que permite a análise dos dados e a sua agrupação em grupos com propriedades comuns. Esse método estrutura os atributos em uma hierarquia, em que o atributo que soluciona a questão está no topo, e os níveis inferiores desse atributo são decompostos, formando uma espécie de "árvore de níveis". A análise é realizada utilizando uma escala de valores, que é usada para atribuir peso a cada atributo. É levada em consideração a compatibilidade entre os atributos e os valores atribuídos às variáveis. O valor final de cada atributo é calculado por meio de uma função aditiva, que contabiliza todos os valores das variáveis e indica a adesão de cada elemento analisado aos atributos (Saaty, 1980).

Morita (1998) descreve algumas etapas para a pesquisa com o método hierárquico, que são apresentadas de forma sintética aqui: 1) Estabelecer critérios em uma hierarquia, do mais global ao mais específico; 2) Avaliar os fatores de decisão (atributos) em cada nível; 3) Determinar o valor de cada atributo e de cada nível, relacionando os efeitos de cada atributo e nível no subsequente. Durante a análise, também é possível verificar a consistência dos dados em cada nível e atributo.

Para Fachin (2001), o método comparado permite realizar uma investigação e explicar fatos por meio de semelhanças e diferenças. Assim, a análise comparada permite observar diferentes realidades em busca de respostas para os problemas. Ainda sobre o tema, King, Keohane e Verba (1994) afirmam que, na pesquisa empírica, é fundamental relatar como os dados foram coletados e criados para possibilitar a replicação da pesquisa científica.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Dessa forma, o desenho metodológico desta pesquisa foi elaborado de maneira a permitir a replicabilidade dos dados levantados. As variáveis utilizadas foram extraídas da Convenção sobre Cibercrime (CONSELHO DA EUROPA, 2001, *online*), um documento internacional de combate à criminalidade na internet que entrou em vigor em 2004 e atualmente possui 65 ratificações em todo o mundo, incluindo os Estados Unidos, que ratificaram o documento em 2007. As variáveis serão baseadas nesse documento devido ao seu caráter pioneiro no combate ao cibercrime, bem como à complexidade de seu texto, que aborda aspectos do direito material, direito processual e políticas públicas que devem ser adotadas pelos governos.

Segundo Clough (2012, 2014), a Convenção de Budapeste é um instrumento importante para o aprimoramento da legislação dos países que a ratificaram. Amalie Weber (2003) afirma que, apesar das críticas e imperfeições, é a melhor solução para os dilemas jurisdicionais envolvendo cibercrimes. Para Hopkins (2003), a iniciativa do Conselho da Europa em produzir a Convenção sobre Cibercrime foi oportuna e bem-vinda para a época em que a Europa se encontrava.

Destarte, foram relacionadas as seguintes variáveis: V1: Criminalizar o ato intencional e ilegítimo de danificar, apagar, deteriorar, alterar ou eliminar dados informáticos. V2: Criminalizar a obstrução ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos. V3: Criminalizar a produção, venda, obtenção para utilização, importação, distribuição ou outras formas de disponibilização de dispositivos ou programas informáticos concebidos ou adaptados essencialmente para permitir a prática de crimes cibernéticos. V4: Criminalizar atos que provoquem a perda de bens a terceiros através de sistemas informáticos. V5: Criminalizar a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infrações previstas na presente Convenção. V6: Garantir que as pessoas coletivas possam ser consideradas responsáveis por crimes estabelecidos conforme a Convenção, quando cometidos em seu benefício por uma pessoa singular agindo tanto individualmente quanto como membro de um órgão da pessoa coletiva. V7: Adoção de medidas legislativas que sejam necessárias para instituir os poderes e os procedimentos

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

previstos na Convenção, para fins de investigação ou procedimento penal. V8: Garantir a obrigatoriedade do provedor de conservar e proteger a integridade dos referidos dados durante um período tão longo quanto necessário, até um máximo de 90 dias, de modo a permitir às autoridades competentes obter sua divulgação. V9: Adoção de medidas que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de conservá-los, a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno. V10: Adoção de medidas que se revelem necessárias para habilitar suas autoridades competentes a apreender ou obter de forma semelhante os dados informáticos relevantes para o combate à criminalidade na internet.

O presente estudo parte da problematização do contraponto entre a quantidade de usuários, ocorrências de cibercrimes e perdas financeiras sofridas pelo Brasil, Estados Unidos e China. Conforme exposto na introdução, o Brasil possui uma população digital mais de dez vezes menor que a quantidade de usuários de internet na China, enquanto as perdas financeiras brasileiras foram apenas três vezes menores que as chinesas (Symantec, 2019). Portanto, esta pesquisa irá trabalhar com as variáveis que afetam a esfera patrimonial. Para isso, foram considerados os dispositivos da Convenção que tratam da responsabilidade das empresas de dados, crimeware-as-a-service e ataques de negação de serviço (DDoS).

No que diz respeito à legislação, no caso brasileiro, foi realizada uma busca no sítio do Planalto (https://legislacao.presidencia.gov.br/) utilizando o termo "internet" com os seguintes filtros: data inicial 01/01/1988, data final 31/12/2020 e os seguintes tipos de atos: CON - Constituição Federal de 1988, DEC - Decreto do Executivo, DEL - Decreto-Lei, EMC - Emenda Constitucional, IN - Instrução Normativa, LCP - Lei Complementar, LEI - Lei Ordinária, PRT - Portaria e RES - Resolução. Foram obtidos 506 resultados, no entanto, foi necessário analisar se o termo "internet" estava presente na ementa da legislação, pois a busca apresentou todos os atos que possuem a palavra "internet" em seu corpo. Portanto, para a presente pesquisa, foram considerados apenas os resultados que continham o termo "internet". Os atos revogados não foram considerados.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Os dados referentes aos Estados Unidos foram retirados da página oficial do Congresso Norte-Americano (https://www.congress.gov/), onde foi realizada uma busca pelo termo "internet" com o filtro "became law" selecionado no campo "Status of legislation", resultando em 524 resultados. No caso americano, foi aplicado o mesmo critério de seleção utilizado no caso brasileiro, considerando-se os atos que possuíam o termo "internet" na ementa e desconsiderando-se os atos revogados.

3 RESULTADOS

A partir dos pressupostos mencionados anteriormente, foi realizada a análise da legislação listada e o processamento dos dados. Foram consideradas as 10 variáveis extraídas da Convenção de Budapeste, e para cada informação obtida, foi atribuído um valor correspondente aos atributos relacionados. Caso a variável correspondesse, foi atribuído o valor um, indicando que o dispositivo existe na legislação. Caso contrário, foi atribuído o valor zero, indicando que o dispositivo não existe na legislação.

Tabela 1

V1- Responsabilizar pelo ato intencional e ilegítimo de danificar, apagar, deteriorar, alterar ou eliminar dados informáticos	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Nos Estados Unidos, a Computer Fraud and Abuse Act (CFAA) estabelece, nos itens A(2), A(4), A(5) e A(7), como crime a invasão de computadores, fraude em computadores, dano a computadores e extorsão por meio de computadores, respectivamente. No Brasil, o artigo 154-A do Código Penal, introduzido pela Lei nº 12.737 de 2012 (conhecida como Lei Carolina Dieckmann), estabelece pena de detenção de três meses a um ano, além de multa, para os delitos mencionados anteriormente.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Tabela 2

V2- Criminalizar a obstrução ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023..

Nos Estados Unidos, a Computer Fraud and Abuse Act (CFAA) estabelece, no item A(6), como crime a interferência não autorizada no tráfego de dados. No Brasil, o artigo 3º da Lei nº 12.737 de 2012 (Lei Carolina Dieckmann) inclui no artigo 266 do Código Penal a punição para "a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública".

Tabela 3

V3- Criminalizar a produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de dispositivo, ou programa informático, concebido ou adaptado essencialmente para permitir a prática de crimes cibernéticos.	
Brasil	Estados Unidos
0	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Nos Estados Unidos, de acordo com o item A(5) da Computer Fraud and Abuse Act (CFAA), é estabelecido como crime a transmissão de um programa, informação, código ou comando que, como resultado dessa conduta, cause danos intencionalmente e sem autorização a um computador protegido. No Brasil, não foi encontrada legislação específica que criminalize a prática de crimeware-as-a-service, que se refere ao comércio de softwares maliciosos.

Tabela 4

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

V4- Criminalizar atos que provoquem a perda de bens a terceiros através de sistemas informáticos.	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Nos Estados Unidos, de acordo com o item A(7) da Computer Fraud and Abuse Act (CFAA), é estabelecido como crime a criminalização das perdas materiais causadas por atos maliciosos na internet. No Brasil, o parágrafo 2 do artigo 154-A da Lei nº 12.737 de 2012 (conhecida como Lei Carolina Dieckmann) estabelece que a pena será aumentada de um sexto a um terço se da invasão resultar prejuízo econômico.

Tabela 5

V5 -Criminalizar a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infrações na presente Convenção.	
Brasil	Estados Unidos
0	0

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Realizando revisão documental, não foi encontrado nenhum dispositivo legal em ambos os países que correspondesse a esta variável.

Tabela 6

V6- Garantir que a pessoas colectivas possam ser consideradas responsáveis por crimes estabelecidas conforme a Convenção, quando cometidas em seu benefício por uma pessoa singular agindo quer individualmente, quer como membro de um órgão da pessoa coletiva.	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Nos Estados Unidos, a Computer Fraud and Abuse Act (CFAA), no item E (12), define que sempre que a CFAA utilizar o termo "pessoa", este refere-se a pessoas físicas e jurídicas. No Brasil, o artigo 3º da Lei nº 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece que tanto pessoas físicas quanto jurídicas são responsáveis pelos dados que possuem.

Tabela 7

V7- Adoção de medidas legislativas que sejam necessárias, para instituir os poderes e os procedimentos previstos na Convenção, para fins de investigação ou de procedimento penal.	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Nos Estados Unidos, a Computer Fraud and Abuse Act (CFAA) possui três dispositivos no item D que delimitam a competência de investigação de cibercrimes, estabelecendo que o United States Secret Service é responsável por investigar tais delitos. No Brasil, o artigo 13, §2º do Marco Civil da Internet prevê que a autoridade policial, administrativa ou o Ministério Público podem requerer cautelarmente a guarda dos registros de conexão por um prazo superior ao previsto no caput, ou seja, por até 1 (um) ano.

Tabela 8

V8- Garantir a obrigatoriedade do provedor de conservar e proteger a integridade dos referidos dados durante um período tão longo quanto necessário, de modo a permitir às autoridades competentes obter a sua divulgação.	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Nos Estados Unidos, a Cybersecurity Act of 2015, na seção 105, nos itens 3-A e 3-B, garante que os provedores devem garantir o acesso das autoridades de investigação aos dados durante todo o processo. No Brasil, o artigo 15 do Marco Civil da Internet (Lei nº 12.965/2014) trata da responsabilidade dos provedores em relação aos dados, e em seus parágrafos 1 e 2 estabelece que o Poder Judiciário pode determinar a duração do período em que os provedores devem assegurar os dados.

Tabela 9

V9- Adoção de medidas que se revelem necessárias para obrigar o responsável pelos dados, ou outra pessoa encarregada de os conservar, a manter segredo sobre a execução dos referidos procedimentos durante o período previsto pelo seu direito interno.	
Brasil	Estados Unidos
1	1

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Nos Estados Unidos, a Cybersecurity Act of 2015, na seção 107, nos itens 1 e 2, trata sobre o sigilo de informações em meio digital. No Brasil, o artigo 42, parágrafo I da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece que os operadores respondem solidariamente pelos danos causados pelo tratamento de dados, quando descumprirem as obrigações da legislação de proteção de dados ou não seguirem as instruções lícitas do controlador.

Tabela 10

V10- Adoção de medidas que se revelem necessárias para habilitar as suas autoridades competentes para apreender ou para obter de forma semelhante os dados informáticos relevantes para o combate da criminalidade na internet.	
Brasil	Estados Unidos
1	1

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Nos Estados Unidos a *Cibersecurity Act of 2012* no item 107 delimita os procedimentos para obtenção de dados pertinentes para investigações criminais. No Brasil o Marco Civil da Internet no artigo 15º, § 2º dispõem que a autoridade policial ou o Ministério Público poderão requerer cautelarmente que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, isto é, por mais de 06 (seis meses).

Tabela 11

Variáveis	Estados Unidos	Brasil
V1	1	1
V2	1	1
V3	1	1
V4	1	1
V5	0	0
V6	1	1
V7	1	1
V8	1	1
V9	1	1
V10	1	1
Resultado	90%	90%

Fonte: MESSIAS, PEQUENO JUNIOR, 2023.

Considerando os resultados obtidos e a equivalência dos dados levantados com as variáveis, verificou-se que a legislação de ambos os países, conferiram o mesmo grau de proteção.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

4 ANÁLISE COMPARADA DE BRASIL E ESTADOS UNIDOS

Com o advento da internet, a onda de cibercrimes, também denominados crimes cibernéticos ou informáticos, estabeleceu-se na comunidade mundial dado o crescimento exponencial do uso da rede.

Neste cenário, o processo de comunicação entre os indivíduos, deslocado para o mundo virtual, torna as relações cada vez mais dinâmicas, dando abertura para o incremento dessa modalidade de crime. Dada a nova realidade social e tecnológica é imprescindível a atualização legislativa para tutelar os novos fenômenos criminais surgidos.

Os Estados Unidos possuem legislação para combater o cibercrime e proteger seus sistemas de informação. Essas leis têm como objetivo garantir a segurança cibernética, prevenir ataques virtuais e responsabilizar os criminosos cibernéticos.

Uma das leis fundamentais nesse contexto é a *Computer Fraud and Abuse Act* (CFAA), promulgada em 1986. Essa lei estabelece uma série de crimes cibernéticos e fornece uma estrutura legal para processar e punir os perpetradores desses atos. A *CFAA* torna ilegal o acesso não autorizado a computadores e sistemas de informação, bem como a obtenção, divulgação ou destruição não autorizada de dados. Ela também proíbe atividades como hacking, phishing, fraude eletrônica e ataques de negação de serviço (Estados Unidos da América, 1986).

Outra legislação importante é o *Cibersecurity Act of 2012*, que tem como objetivo fortalecer a segurança cibernética do país. Essa lei promove a colaboração entre o governo, o setor privado e a comunidade acadêmica para compartilhar informações sobre ameaças cibernéticas e desenvolver medidas de proteção mais eficazes. O *Cibersecurity Act of 2012* também estabelece diretrizes para a proteção de infraestruturas críticas, bem como para a resposta a incidentes de segurança cibernética.

O *Cybersecurity Act of 2012* é uma legislação importante promulgada nos Estados Unidos com o objetivo de fortalecer a segurança cibernética e proteger as infraestruturas críticas do país. Foi um marco significativo no reconhecimento da

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

importância da segurança digital e na implementação de medidas para combater as ameaças cibernéticas.

Esta lei teve como principal objetivo estabelecer políticas e diretrizes para a proteção das redes de informação e sistemas de computadores utilizados pelo governo federal e setores considerados críticos, como energia, comunicações, transporte e serviços financeiros. Seu enfoque estava na prevenção de ataques cibernéticos, na identificação e resposta a incidentes de segurança, bem como na promoção da colaboração entre o setor público e o setor privado.

Uma das principais disposições do *Cybersecurity Act of 2012* foi a criação de padrões de segurança cibernética e requisitos de relatórios para as infraestruturas críticas. Esses padrões visavam garantir a proteção adequada dos sistemas de tecnologia da informação e estabelecer medidas para prevenir e responder a incidentes de segurança cibernética.

Além disso, a legislação também promoveu a colaboração entre o governo, a indústria e a comunidade acadêmica por meio da troca de informações sobre ameaças cibernéticas, práticas recomendadas de segurança e desenvolvimento de capacidades de resposta conjunta.

O *Cybersecurity Act of 2012* também trouxe disposições relacionadas à proteção da privacidade e dos direitos individuais. Buscou equilibrar a segurança cibernética com a necessidade de preservar a liberdade e a confidencialidade das informações pessoais. A lei estabeleceu diretrizes claras para o tratamento adequado das informações coletadas e promoveu a transparência e a responsabilização no uso desses dados.

Além dessas leis, os Estados Unidos possuem outras legislações que abordam aspectos específicos do cibercrime. Por exemplo, a *Identity Theft and Assumption Deterrence Act* (ITADA) criminaliza o roubo de identidade e estabelece penas para os infratores. *A Children's Online Privacy Protection Act (COPPA)* protege a privacidade das crianças online e regula a coleta e o uso de informações pessoais de menores de idade.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Além disso, o país também possui agências governamentais especializadas na segurança cibernética, como a *Cybersecurity and Infrastructure Security Agency (CISA*) e o *Federal Bureau of Investigation (FBI),* que investigam e combatem crimes cibernéticos em conjunto com outras entidades governamentais e setores relevantes.

O Brasil, por sua vez, também apresenta vasta legislação sobre o tem, a seguir são apresentados exemplos de leis aplicáveis aos crimes virtuais, utilizando-se de paráfrases para expressar a similaridade com os dispositivos legais originais: Calúnia: De acordo com o artigo 138 do Código Penal, é considerado calúnia quando alguém atribui falsamente a outra pessoa a prática de um crime. A pena para esse delito é de detenção de seis meses a dois anos, além de multa; Difamação: O artigo 139 do Código Penal trata da difamação, que ocorre quando alguém atribui a outra pessoa um fato ofensivo à sua reputação. A pena para esse crime é de detenção de três meses a um ano, acompanhada de multa. No entanto, é importante mencionar que há uma exceção da verdade, que se aplica somente quando o ofendido é funcionário público e a ofensa está relacionada ao exercício de suas funções; Injúria: O crime de injúria está previsto no artigo 140 do Código Penal. Ele ocorre quando alguém ofende a dignidade ou o decoro de outra pessoa, por meio de palavras, gestos ou atitudes. A pena para esse delito varia de acordo com a gravidade da ofensa e pode resultar em detenção ou multa.

Além dos crimes contra a honra, existem outras normas que também são aplicáveis aos crimes virtuais, tais como: Ameaça (artigo 147 do Código Penal); Furto (artigo 155 do Código Penal); Dano (artigo 163 do Código Penal); Apropriação indébita (artigo 168 do Código Penal); Estelionato (artigo 171 do Código Penal); Violação ao direito autoral (artigo 184 do Código Penal); Pedofilia (artigos 240 e 241 da Lei nº 8.069/1990 - Estatuto da Criança e do Adolescente); Pornografia Infantil (artigo 234); Crime contra a Propriedade Industrial (artigos 183 e seguintes da Lei nº 9.279/1996); Interceptação de Comunicações de Informática (artigo 10 da Lei nº 9.296/1996); Interceptação de e-mail Comercial ou Pessoal (artigo 10 da Lei nº 9.296/1996); Crimes contra software - Pirataria (artigo 12 da Lei nº 9.609/1998).

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Nos artigos 240 e 241 do Estatuto da Criança e do Adolescente (Lei 8.069/1990), estão estabelecidas as infrações relacionadas à pedofilia. O artigo 240 tipifica a produção, reprodução, direção, fotografia, filmagem ou registro, por qualquer meio, de cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. A pena para esse crime é de reclusão de 4 a 8 anos, além de multa. O parágrafo 1º do artigo 240 também estabelece que as mesmas penalidades se aplicam a quem age como intermediário, facilitador ou recrutador de crianças ou adolescentes nesse tipo de cena.

Já o artigo 241 trata da venda ou exposição à venda de fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. A pena prevista é de reclusão de 4 a 8 anos, acompanhada de multa.

No que diz respeito ao artigo 171 do Código Penal, ele aborda o crime de estelionato, que consiste em obter, para si ou para outrem, vantagem ilícita em prejuízo alheio, por meio de artifício, ardil ou qualquer outro meio fraudulento. A pena para esse delito é de reclusão de 1 a 5 anos, além de multa.

O artigo 184 do Código Penal prevê a violação dos direitos autorais e dos direitos conexos como crime. Ele abrange a violação de direitos de autor, como reprodução não autorizada de obras protegidas, e ações que afetam esses direitos. A pena para esse tipo de infração varia de detenção de 3 meses a 1 ano, ou multa.

A Lei nº 7.232/1984 foi uma das primeiras leis voltadas para crimes virtuais no Brasil. Ela estabeleceu diretrizes e princípios da Política Nacional de Informática (PNI) por meio da criação do Conselho Nacional de Informática (CONIN), como mencionado por Barreto (2017). Posteriormente, surgiram outras legislações com o objetivo de proteger bens jurídicos no âmbito virtual e suas relações. A Lei nº 7.646/1987, que tratava da comercialização de programas de computador e apoio intelectual no Brasil, foi revogada pela Lei nº 9.609/1998, que reconheceu como crime as transgressões nessa área (Barreto, 2017).

A Lei nº 12.737/12, conhecida como Lei de crimes cibernéticos, trouxe uma importante contribuição ao sistema jurídico penal brasileiro ao introduzir o crime de "Invasão de Dispositivo Informático". Esse delito consiste na ação de invadir um dispositivo informático pertencente a terceiros, independentemente de estar conectado

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

ou não à rede de computadores. A invasão ocorre mediante a violação indevida de mecanismos de segurança com o intuito de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo. Além disso, também configura crime a instalação de vulnerabilidades com o propósito de obter vantagem ilícita.

Essa lei é de extrema importância para lidar com os desafios e as ameaças impostas pelo ambiente digital, estabelecendo punições para condutas que comprometam a segurança e a privacidade das informações armazenadas em dispositivos eletrônicos. Com a criminalização dessa prática, busca-se garantir a proteção dos dados pessoais, preservar a integridade dos sistemas computacionais e combater as ações de indivíduos mal-intencionados que buscam se beneficiar ilegalmente por meio da invasão de dispositivos informáticos alheios.

A Lei nº 12.737/12, é também conhecida como "Lei Carolina Dieckmann", recebeu esse nome em referência a um caso amplamente divulgado na mídia envolvendo a atriz brasileira Carolina Dieckmann, que teve seu dispositivo eletrônico invadido e suas fotos íntimas divulgadas sem autorização.

Ao introduzir o crime de "Invasão de Dispositivo Informático", essa legislação contribuiu para fortalecer a proteção dos direitos individuais no ambiente virtual, incentivando a segurança cibernética e a responsabilização daqueles que praticam condutas ilegais nesse contexto. A partir dessa lei, é possível responsabilizar criminalmente os invasores de dispositivos informáticos, promovendo a conscientização sobre a importância da segurança digital e garantindo a justiça na esfera virtual.

O Marco Civil da Internet, Lei nº 12.965/14, aborda importantes questões relacionadas à proteção e regulação do ambiente digital. Ela estabelece diretrizes para o uso da Internet no Brasil, tratando de temas como a neutralidade da rede, a proteção de dados, o registro de conexão e a responsabilidade por danos. Um dos aspectos relevantes é a exigência de uma requisição judicial para acesso às informações, garantindo a privacidade e a segurança dos usuários. O Marco Civil da Internet assegura o exercício da cidadania nos meios digitais, protegendo os direitos e garantias fundamentais dos indivíduos nesse contexto.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

Já a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/18, foi promulgada com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, bem como a formação da personalidade de cada indivíduo. Essa legislação abrange o tratamento de dados pessoais, sejam eles em formato físico ou digital, realizado por pessoas físicas ou jurídicas, sejam elas de direito público ou privado. A LGPD engloba um amplo conjunto de operações que envolvem dados pessoais, sejam elas realizadas de forma manual ou digital.

Os direitos à privacidade e à proteção de dados pessoais são fundamentais e estão elencados no artigo 5º da Constituição Federal. A Emenda Constitucional nº 115/2022, de autoria da ex-senadora Simone Tebet, acrescentou o direito à proteção de dados pessoais ao rol de direitos e garantias fundamentais do cidadão. Além disso, fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Essa emenda proporciona maior segurança jurídica no país quanto à aplicação da LGPD, tornando o Brasil mais atrativo para investimentos internacionais.

Apesar dos direitos mencionados estarem garantidos pela legislação vigente, é importante destacar que ainda existem lacunas legislativas que podem dificultar ou até mesmo impossibilitar a aplicabilidade desses direitos de maneira efetiva, gerando insegurança jurídica. Portanto, é necessário continuar aprimorando as normas e regulamentações para garantir uma proteção adequada dos direitos à privacidade e à proteção de dados pessoais.

De fato, a Lei 12.737/2012, representou um marco legislativo importante no combate aos cibercrimes. Antes dessa lei, muitos crimes cometidos no ambiente virtual não eram devidamente tipificados na legislação, o que gerava lacunas na responsabilização dos infratores. A lei trouxe uma definição mais precisa e abrangente dos delitos cometidos por meio de computadores e da internet, preenchendo essa lacuna.

Os crimes informáticos próprios são aqueles cometidos especificamente contra dados, programas ou a estrutura física de sistemas computacionais. Eles demandam modalidades penais específicas, dada a sua natureza peculiar. Exemplos desses

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

crimes são as fraudes eletrônicas, invasão de dispositivos informáticos, desvio de DNS e instalação de vulnerabilidades em sistemas para obter acesso indevido a dados.

É importante destacar que a ausência de previsão legal para a punição de certas condutas praticadas no meio virtual impede sua responsabilização no âmbito do Direito, devido ao princípio da legalidade penal. O princípio nullum crimen, nulla poena sine lege, expresso no

Necessário pontuar que a ausência de previsão legal para a punição de certas condutas praticadas no mundo virtual impede a sua responsabilização no plano do Direito, dada a inadmissibilidade de utilização da analogia *in malam partem* no Direito Penal e a estrita obediência ao princípio constitucional penal da legalidade, expresso no brocardo latino *nullum crimen, nulla poena sine lege* (Mirabete & Fabbrini, 2012).

No âmbito legislativo, o Marco Civil da Internet (Lei nº 12.965/2014) foi elaborado para regular as relações no ambiente digital. Essa lei estabelece fundamentos e princípios que devem ser considerados no uso da rede, buscando garantir direitos e responsabilidades dos usuários. O Marco Civil da Internet também aborda questões como neutralidade da rede, proteção de dados, registro de conexão e responsabilidade por danos, contribuindo para a regulamentação do ambiente virtual.

A referida lei alterou alguns artigos do Código Penal de modo a abranger a internet como um novo meio de ocorrência, a exemplo dos arts. 154-A e 154-B, versando estes sobre invasão de dispositivos, acrescentando ainda novos mecanismos previstos nos artigos 266 e 298.

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública. § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2o Aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública.
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. Falsificação de cartão. Parágrafo único. Para fins do disposto no

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

> caput, equipara-se a documento particular o cartão de crédito ou débito (Brasil,2021, *online*).

O avanço legislativo sobre o universo virtual tem se revelado uma tendência em todo o mundo. Nesse sentido, a Convenção de Budapeste, um tratado internacional firmado no contexto europeu, abrange aspectos do Direito Penal e Processo Penal relacionados aos crimes praticados por meio da internet e suas repercussões no âmbito jurídico. A Convenção entrou em vigor em 1º de julho de 2004.

No Brasil, em 2018, a Presidência da República instituiu a Política Nacional de Segurança da Informação (Decreto 9.637, de 26 de dezembro de 2018), estabelecendo aspectos de governança e segurança da informação. Esse decreto lista objetivos e princípios da segurança e defesa cibernética brasileira. Um dos principais instrumentos estabelecidos pela PNSN foi o Comitê Gestor de Segurança da Informação, responsável por assessorar o Gabinete de Segurança Institucional em atividades relacionadas à segurança da informação (Brasil, 2018).

Outro aspecto relevante da PNSN foi a atribuição de responsabilidade na elaboração de políticas públicas referentes à segurança da informação ao GSI, que atualmente possui status de ministério. Essa responsabilidade também é compartilhada com o Ministério da Defesa, que desempenha um papel fundamental na defesa cibernética (art. 13º, inciso II).

Na seção IV do Decreto 9.637, é estabelecida a atuação dos órgãos e entidades da administração pública federal, os quais devem implementar a PNSN e executar uma série de ações para garantir a segurança da informação.

5 CONSIDERAÇÕES FINAIS

Em termos teóricos, o principal objetivo deste artigo foi analisar a proteção legal em matéria de cibercrimes no Brasil e nos Estados Unidos. Os resultados sugerem uma similaridade significativa nas leis adotadas por ambos os países. No entanto, os

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

resultados indicam que a legislação por si só não é suficiente para explicar as diferenças observadas na prática

É evidente que uma norma isolada não tem o poder de modificar a realidade de forma expressiva. A efetividade da proteção legal contra cibercrimes depende também de práticas institucionais, políticas de combate e governança da web. A proteção contra cibercrimes requer uma abordagem abrangente, que envolva não apenas a criação de legislação adequada, mas também a implementação de mecanismos de prevenção, detecção e resposta eficientes. Portanto, é fundamental considerar a implementação de políticas públicas e a adoção de medidas adequadas para fortalecer a proteção contra cibercrimes em ambos os países.

É inegável que uma norma isolada é incapaz de modificar a realidade de forma expressiva, sendo necessárias práticas e políticas públicas que a implementem, aperfeiçoando a efetividade do sistema de proteção.

Portanto, conclui-se que a análise comparativa entre a proteção legal em matéria de cibercrimes no Brasil e nos Estados Unidos não revelam diferenças significativas. Nesse sentido, é importante ressaltar que a efetividade dessa proteção vai além das normas legais, dependendo também de práticas institucionais, políticas de combate e governança da web. A implementação de políticas públicas e a adoção de medidas adequadas são fundamentais para fortalecer a proteção contra cibercrimes em ambos os países.

REFERÊNCIAS

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei n. 12.737/2012, março 2017**. Disponível em: <http://www.conteudojuridico.com.br/consulta/artigos/49678/crimescibernetico s-soba-egide-da-lei-12-737-2012>. Acesso em: 27. jun. 2023.

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. **Decreto nº 9.637**, *de 26 de dezembro de 2018*. Planalto, Brasília, 24 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm> Acesso em: 26 de jan. de 2021.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

BRASIL**. Lei nº 12.737**, **de 30 de novembro de 2012.** Planalto, Brasília, 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 26 de jan. de 2021.

BRASIL**. Lei nº 12.965, de 23 de abril de 2014**. Planalto, Brasília, 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 26 de jan. de 2021.

CASTRO, C. R. **A. Crimes de informática e seus aspectos processuais.** 2. ed. Rio de Janeiro, 2003.

CETIC. **Domicílios com acesso a internet**. Cetic, São Paulo, 2019. Disponível em: <https://www.cetic.br/pt/tics/domicilios/2019/domicilios/A4/> Acessado em: 26 de jan. de 2021.

CLOUGH, J.. The Council of Europe Convention on cybercrime: definingcrime'in a digital world. **Criminal Law Forum**. Vol. 23, No. 4, pp. 363-391. Springer Netherlands. 2012.

CLOUGH, J. A world of difference: the Budapest convention of cybercrime and the challenges of harmonisation**. Monash UL Rev**., *40*, 698.2014.

CONSELHO DA EUROPA. **Convenção sobre Cibercrimes**. Budapeste, 2001. Disponível em: <https://rm.coe.int/16802fa428> Acessado em: 28 de nov de 2020.

COSTA, Fernando José da. **Locus delicti nos crimes informáticos**. 2011. Tese de Doutorado. Faculdade de Direito da Universidade de São Paulo. Disponivel em: <https://www.teses.usp.br/teses/disponiveis/2/2136/tde-24042012-112445/pt-br.php> Acessado em: 11 de jan 2021.

ESTADOS UNIDOS DA AMÉRICA. **Computer Fraud and Abuse Act of 1986.** Disponível em: **<** https://www.congress.gov/bill/99th-congress/house-bill/4718>. Acessado em: 27 jun. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Cybersecurity Act of 2012.** Disponível em: **<** https://www.congress.gov/bill/112th-congress/senate-bill/2105>. Acessado em: 27 jun. 2023

FACHIN, Odília. **Fundamentos de metodologia.** São Paulo: Saraiva. 2001.

HOPKINS, S. L. **Cybercrime convention: a positive beginning to a long road ahead.** J. High Tech. L., *2*, 101. 2003.

ISSN nº 2359-0106 Vol. 10, n. 2, 2023.

https://doi.org/10.20873/uft.2359-0106.2020.v10n2.p70-92

INTERPOL. **Cybercrimes**. 2020. Disponível em: <https://www.interpol.int/Crimes/Cybercrime>. Acesso em: 03 jan 2021.

KING,G.; KEOHANE, R.; VERBA, S. **Design social inquiry: scientific inference in qualitative research**. Princeton: Princeton University Press, 1994.

LIMA, P. M. F**. Crimes de computador e segurança computacional**. 2. ed. São Paulo: Atlas, 2011.

MIRABETE, J. F.; FABBRINI, R. N**. Manual de direito penal: parte geral**. São Paulo: Atlas, 2019.

MORITA, H. **Revisão do método de análise hierárquica - MAH (AHP- Analytic Hierarchy Process)**. Dissertação (Mestrado) - Escola Politécnica, Universidade de São Paulo, 1998.

SAATY, T. **The analytic hierarchy process.** New York; McGraw-Hil, 1980.

SIMAS, D. V. **O cibercrime.** Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

SYMANTEC**. Norton cyber security insights report**. Disponivel em: <https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2017/#:~:text=Uncover%20the%20discrepancies%20behind%20consumers,21%2C000%20consumers%20in%2020%20countries.>. Acesso em 11 de set. 2020.

WEBER, A. *The Council of Europe's Convention on Cybercrime*. **Berkeley Technology Law Journal***,* 2003.