INSTITUTO BRASILIENSE DE DIREITO PÚBLICO – IDP
ESCOLA DE DIREITO DE BRASÍLIA – EDB
CURSO DE GRADUAÇÃO EM DIREITO

PATRÍCIA BERTO BUANI

A COMPATIBILIDADE ENTRE O ORDENAMENTO JURÍDICO BRASILEIRO E A CONVENÇÃO SOBRE CIBERCRIMES.

BRASÍLIA
JULHO/2020

PATRÍCIA BERTO BUANI

A COMPATIBILIDADE ENTRE O ORDENAMENTO JURÍDICO BRASILEIRO E A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIMES.

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito para conclusão do curso de Direito e obtenção do título de bacharel em Direito pela Escola de Direito e Administração Pública - EDAP/IDP.

Orientadora: Miriam Wimmer

BRASÍLIA

JULHO/2020

PATRÍCIA BERTO BUANI

A COMPATIBILIDADE ENTRE O ORDENAMENTO JURÍDICO BRASILEIRO E A CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIMES.

Trabalho de Conclusão de Curso apresentado à banca examinadora como requisito para conclusão do curso de Direito e obtenção do título de bacharel em Direito pela Escola de Direito e Administração Pública - EDAP/IDP.

Orientadora: Miriam Wimmer

Brasília, julho de 2020.

Professora Miriam Wimmer
Membro da Banca Examinadora

Professor Guilherme Pereira Pinheiro
Membro da Banca Examinadora

Professor Alexandre Sankievicz
Membro da Banca Examinadora

RESUMO

A Internet, por meio da rede mundial de computadores, se torna um importante instrumento no cotidiano dos indivíduos mundialmente. Traz consigo os benefícios e os malefícios da ferramenta. Por isso é de suma importância a tipificação de crimes cibernéticos e uma melhor definição e conceituação do que são cibercrimes e quais as formas possíveis de cometê-los. Este trabalho examina em que medida a legislação brasileira atual é harmônica com a Convenção sobre Cibercrimes, mais conhecida como Convenção de Budapeste, e de que maneira o Brasil pode ser considerado integrado ao esforço global realizado no combate aos cibercrimes. Trata-se de um tema importante não só do ponto de vista político internacional, social e jurídico, mas também sob o aspecto econômico, já que diversos países e empresas, para manterem relações com o Brasil, preocupam-se com a higidez e com a segurança proporcionada pelo sistema jurídico nacional. Visando buscar soluções no combate ao cibercrime, o presente trabalho perpassa por um contexto histórico, tanto na Europa, como no Brasil, buscando entender de que maneira a Convenção de Budapeste seria boa ou ruim para o nosso ordenamento jurídico e se o Brasil é visto, perante os outros países, integrado ao esforço global de combate ao cibercrimes.

PALAVRAS-CHAVE: Crimes virtuais. Cibercrimes. Rede mundial de computadores. Convenção de Budapeste. Cronologia legislativa. Lei Carolina Dieckmann. Marco Civil da Internet.

Sumário

INTRODUÇÃO

A Internet é um instrumento fundamental para o desenvolvimento e organização de todos os países, e se tornou essencial para o funcionamento da sociedade. São incontáveis benefícios e vantagens que a rede mundial de computadores proporciona. Mas, assim como a Internet traz benefícios aos usuários, também pode ser usada para o cometimento de atos ilícitos diversos.

Assim, nasce o termo cibercrimes. O termo pode ser usado tanto para tipificar crimes que já existiam, mas agora cometidos no ambiente virtual, bem como para designar os crimes inéditos, que começaram a surgir com o advento da Internet. Por esse motivo se torna imprescindível a tipificação dos crimes cibernéticos e uma melhor conceituação do que são cibercrimes e quais as possíveis formas de cometê-los.

O presente estudo surge, então, dos questionamentos e indagações feitas a respeito desses cibercrimes. Buscando examinar em que medida a legislação brasileira atual é harmônica com a Convenção de Budapeste, e de que maneira o Brasil o integra o esforço global realizado no combate aos cibercrimes, uma vez que, tornando-se membro da referida Convenção, se tornaria parte de um regime internacional de combate a esta modalidade de delitos, o que facilitaria na cooperação internacional nos casos de crimes transnacionais. Evidencia-se um tema importante não só do ponto de vista político internacional, mas também sob o aspecto social, jurídico, e também econômico, já que diversos países e empresas para manterem relações com o Brasil, preocupam-se com a higidez e a segurança proporcionada pelo sistema jurídico nacional.

Este trabalho, pretende, portanto, analisar a compatibilidade da legislação brasileira com a Convenção de Budapeste e avaliar a existência de eventuais dificuldades jurídicas para a adesão do Brasil a esse tratado internacional. Para tanto, o trabalho examinará de que forma o Brasil pode ser visto integrado ao esforço de combate internacional aos cibercrimes.

No primeiro capítulo é feito um estudo a respeito da história da Internet e a conceituação do termo cibercrime, fazendo a importante diferenciação entre crimes cibernéticos próprios e impróprios. Já no segundo capítulo o texto perpassa por organizações como a OCDE (Organização para a Cooperação e Desenvolvimento Econômico), a Interpol, o grupo econômico intitulado de G8 e o Conselho da Europa, organismo internacional fundamental no debate acerca da Convenção de Budapeste, visando apresentar o cenário europeu sobre cibercrimes da época.

No capítulo três é feita uma cronologia da legislação brasileira, evidenciando diplomas legais que buscaram, civil ou penalmente, a responsabilização de indivíduos que praticavam condutas ilícitas no ambiente virtual. Primeiramente é apresentado o projeto de lei 84/1999, mais conhecido como AI-5 Digital. Este projeto de lei encontrou dificuldades em ser aprovado no Congresso Nacional

por sua rigidez e pontos dúbios. Posteriormente, após diversos artigos serem retirados do texto original, o projeto de lei batizado de Lei Azeredo se transformou na Lei 12.735/2012.

No mesmo dia e no mesmo ano que a lei Azeredo foi aprovada, a Lei 12.737/2012, mais conhecida como Lei Carolina Dieckmann, também foi sancionada. Esse dispositivo criou um novo tipo penal: a invasão de dispositivo informático, além de incluir não só a interrupção telegráfica e telefônica, mas também a informática, a telemática e a de informação de utilidade pública. Por fim essa lei equiparou o cartão de crédito e débito a documento pessoal.

Ainda no capítulo três é abordado o tema Marco Civil da Internet ou, como é conhecido, a Constituição da Internet Brasileira, sendo um dos dispositivos civis mais importantes relacionados ao ambiente cibernético pois surgiu como meio de solução para as lacunas legislativas existentes. Por fim, o capítulo finaliza com um dos temas mais atuais relacionados à segurança cibernética, a Estratégia Nacional para Segurança Cibernética - E-Ciber, aprovada pelo Decreto n. 10.222 de 2020.

O presente estudo se encerra no capítulo quatro, no qual é possível, após uma apresentação do contexto histórico mundial e de um apanhado cronológico legislativo, perceber em que medida a legislação brasileira atual se harmoniza com a Convenção de Budapeste, e de que maneira o Brasil pode ser integrar ao esforço global realizado no combate aos cibercrimes. Trata-se de tema importante não só sob o aspecto social, jurídico e político internacional, mas também sob o aspecto econômico, já que diversos países e empresas, para manterem relações com o Brasil, preocupam-se com a higidez e a segurança proporcionada pelo sistema jurídico nacional.

1. CIBERCRIME

Com o fim da Segunda Guerra Mundial, diversas tecnologias foram criadas, desenvolvidas e aprimoradas, porém, por muito tempo, a acessibilidade a tais instrumentos era restrita ao uso militar. Pierry Lévy[1] explica que "a informática servia aos cálculos científicos, às estatísticas dos Estados e das grandes empresas ou tarefas pesadas de gerenciamento (folhas de pagamento)".

A Internet que conhecemos como um meio acessível à população surgiu na década de 90, vindo a se massificar a partir de então. Há mais ou menos quinze anos que a Internet conquista rapidamente espaços cada vez maiores na sociedade. Em um momento inicial, chegou-se a acreditar que esse espaço fosse “terra de ninguém”.

[1] LÉVY, Pierre; **Cibercultura**. São Paulo: Ed. 34, 1999, p. 29.

Isso facilitou o cometimento de crimes *online* e o aparecimento de novos delitos, fazendo surgir o termo cibercrime. O direito, visando acompanhar as demandas que surgem na sociedade, busca regular esse ciberespaço que parecia tão abstrato e distante de nossa realidade.

Lévy[2] define o ciberespaço como "o espaço de comunicação aberto pela interconexão mundial de computadores e das memórias dos computadores''.

> O ciberespaço (que também chamarei de rede) é o mais novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infra estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.[3]

Com o surgimento dessa rede de computadores interligados mundialmente, a informação se tornou rápida, versátil, instantânea e passageira. A facilidade com que as informações vêm e vão deram um novo sentido em diversas áreas. Cartas entraram em extinção, o jornal já não é mais o mesmo, a televisão e os meios de comunicação em geral se modernizaram. Distancias foram encurtadas, bastava apenas um clique para se estar em qualquer lugar do mundo. É uma ideia muito atrativa e por muitos anos se acreditou não haver regras ou limites.

O direito, buscando acompanhar as inovações tecnológicas, visou proteger princípios fundamentais, resguardar direitos e assegurar a efetividade da tutela jurisdicional no espaço cibernético. Foi nesse contexto que, no âmbito internacional, surgiu a convenção de Budapeste e, no Brasil, foram aprovadas diversas leis no âmbito penal e civil com o objetivo de suprir vácuos legislativos decorrentes das novas formas de relação social surgidas a partir do século XX. Entraram no radar dos legisladores de todo mundo os chamados crimes cibernéticos.

Para Tateoki[4], podem ser considerados crimes cibernéticos:

> [...] isto é que ocorra em meio digital: crimes contra a honra ameaçam, induzimento e instigação ou auxilio a suicídio, furto, falsificação de documentos, estelionato, espionagem industrial, violação de segredo, apologia de crime, racismo, atentado a serviço de utilidade pública, pornografia infantil, corrupção de menores em salas de bate papo de internet, violação de direitos de autor, inserção de dados falsos em sistema de informações, crimes contra equipamentos de votação, invasão de dispositivo informático.

Desde a década de 90, o legislador se deparou com uma nova realidade no Direito, diferentemente daquela que estava acostumado a legislar. Surgiu um novo ramo, o Direito Digital, Direito Eletrônico, Direito Cibernético, ou, nas palavras do pesquisador Marcio Pinto, Direito da

---

[2] LÉVY, Pierre; **Cibercultura**. São Paulo: Ed. 34, 1999, p. 92.
[3] LÉVY, Pierre; **Cibercultura**. São Paulo: Ed. 34, 1999, p. 15.
[4] TATEOKI, Victor. **Classificação dos Crimes Digitais**. Disponível em: <https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais>. Acesso em: 13 out. 2019.

Informática[5]. O mundo físico se tornou virtual, as digitais viraram IP's e encontrar o responsável por condutas ilícitas se tornou muito mais difícil quando se está a lidar com indivíduos capazes de burlar sistemas informáticos sem deixar rastros.

A partir de então, condutas já previstas pelo Código Penal passaram a ser praticadas também no ambiente virtual. Assim, costuma-se chamar de crimes cibernéticos impróprios[6] aqueles crimes que já possuíam tipificação legal e apenas passaram a possuir um novo meio para seu cometimento, como, por exemplo, a fraude, o furto, o estelionato, a disseminação de pornografia infantil, a apologia ou incitação ao crime e aos crimes contra a honra, tais como difamação, injúria, calúnia, racismo ou xenofobia.

É o que diz Almeida[7], para quem tais crimes são praticados:

> "[…] para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado, crimes, portanto que já tipificados que são realizados agora com a utilização do computador e da rede, utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado como no caso de crimes […]".

Porém, além dos cibercrimes impróprios, em que os crimes já existiam sem a necessidade de um computador, surgiram novos crimes, os quais não estavam previstos em legislação brasileira alguma e feriam direitos e garantias fundamentais. Tais crimes eram necessariamente praticados por meio de sistemas informatizados. São os chamados crimes cibernéticos próprios.

Novamente remetendo à definição de Almeida[8], os crimes cibernéticos próprios "[…] são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime".

Surgiam então os cibercrimes, ou crimes virtuais, ou crimes digitais, ou crimes informáticos, dentre outras terminologias. A dificuldade estava na detecção dos crimes e na aplicação da lei, do Código Penal e de Processo Penal, pois para as condutas criminosas já previstas na legislação era de fácil aplicação a analogia, porém naqueles crimes que surgiam e só eram passíveis de serem

---

[5] PINTO, Marcio. **O Direito da internet: o nascimento de um novo ramo jurídico.** Disponível em: <http://jus.com.br/revista/texto/2245>. Acesso em: 03 mar 2020.

[6] BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012**. Revista Âmbito Jurídico**.** Disponível em: <https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>. Acesso em: 07 maio 2020.

[7] ALMEIDA, Jéssica de Jesus. **Crimes cibernéticos**. Periódicos Grupo Tiradentes, p. 225. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>. Acesso em 07 maio 2020.

[8] ALMEIDA, Jéssica de Jesus. **Crimes cibernéticos**. Periódicos Grupo Tiradentesp. 224. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>. Acesso em 07 maio 2020.

praticados no ambiente virtual havia uma grande lacuna na legislação quanto a responsabilização do autor de um crime virtual.

O cibercrime seria qualquer conduta ilegal praticada mediante algum dispositivo informático estando ele conectado ou não a rede mundial de computadores. Nesse sentido assevera Aldemario Araujo Castro:

> [...] são denominados de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados). [9]

Além da dificuldade em enquadrar o delito em alguma previsão legal, há uma grande lacuna em relação ao estabelecimento de critérios para definir a jurisdição competente para processar um cibercrime pois, por ser praticado por meio de uma ferramenta global e de fácil propagação, o delito em questão pode, muitas vezes, não possuir fronteiras geográficas.

Com isso alguns tratados internacionais e dispositivos de lei foram criados e alterados. O primeiro tratado internacional que buscou tipificar os crimes cometidos no ambiente cibernético foi a Convenção sobre Cibercrimes, à qual o Brasil ainda não aderiu.

2. A CONVENÇÃO DE BUDAPESTE E A NECESSIDADE DE COOPERAÇÃO INTERNACIONAL NO COMBATE AO CIBERCRIME

Com a chegada da Era da Informação e dos cibercrimes, foi necessário se preocupar com condutas ilícitas já existentes e novas condutas praticadas no ciberespaço, que alteraram limites geográficos e ressignificaram fronteiras. A competência e a jurisdição já não eram fáceis de se definir ao se tratar de crimes transnacionais. Assim, restou clara e evidente a necessidade de uma cooperação jurídica internacional entre os países para uma melhor aplicação do Direito e para a resolução de conflitos.

É nesse cenário que surge a Convenção sobre Cibercrimes, celebrada no ano de 2001 e está em vigor desde 2004[10]. Ou seja, desde 2001 que já havia na Europa e em diversos países do mundo,

---

[9] CASTRO, Aldemario. **A internet e os tipos penais que reclamam ação criminosa em público.** Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf>. Acesso em 03 mar. 2020.

[10] **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em 03 mar. 2020.

normas internacionais a respeito dos crimes cibernéticos. Entretanto essa preocupação data desde muito antes disso.

Passa-se, a seguir, a descrever algumas das organizações em que esse tema já vinha sendo objeto de debates.

2.1 CONSELHO DA EUROPA

O Conselho da Europa é um organismo internacional que foi criado em 1949, pós Segunda Guerra Mundial, com o objetivo de unir os diversos países europeus em um estado de paz. Seu órgão mais conhecido é o Tribunal Europeu de Direitos do Homem. Vale ressaltar que o Conselho da Europa não se confunde com a União Europeia, onde o primeiro é uma organização internacional e o segundo produto de um processo de integração econômica e social, que evoluiu para um sistema de governo colaborativo. Por sua natureza, o Conselho da Europa tende a ser bem mais flexível pois os tratados por eles criados são abertos à participação de todo o globo terrestre, e não só daqueles países que fazem parte do continente europeu.[11]

Com isso podemos perceber que diversas organizações, principalmente na Europa, já se demonstravam preocupadas há décadas com os rumos que a rede mundial de computadores poderia vir à tomar, os limites geográficos e as penalidades aplicáveis. Mas foi na década de 90 com a popularização da internet e com o surgimento do ciberespaço e consequentemente a cibercriminalidade, facilitador e condutor para o cometimento de crimes, sejam eles transnacionais ou não, próprios ou impróprios que surgiu o desafio de delimitar competências e jurisdições para a aplicação do Direito.

Em 1976 ocorre na Europa uma Conferência sobre Aspectos Criminológicos da Criminalidade Econômica quando o Conselho da Europa descreveu e introduziu diversos cibercrimes.[12]

2.2 INTERPOL

Mas, vale lembrar que muito antes disso, em 1923, foi criada a Interpol, organização internacional que facilita a cooperação policial mundial para o controle do crime[13] e para auxiliar na troca de informações e dados entre os sistemas policiais dos diversos Estados signatários.

---

[11] VERONESE, Alexandre. **Cooperação jurídica e proteção de dados pessoais – A necessidade de inserção do Brasil nos tratados do Conselho da Europa.** Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/cooperacao-juridica-e-protecao-de-dados-pessoais-12042019>. Acesso em 08 maio 2020.

[12] SCHJOLBERG, Stein. **The History of Global Harmonization on Cybercrime Legislation**

[13] GOMES, Rodrigo. **Interpol.** Disponível em <https://www.infoescola.com/geografia/interpol/> . Acesso em 24 jun. 2020.

Em 1979 esta organização internacional enfrentou o tema crimes cibernéticos em uma Conferência, que ocorreu em Paris no ano de 1979 onde já havia preocupação com a ideia de que "a natureza da criminalidade informática é internacional, devido ao constante aumento das comunicações por telefone, satélites, entre os diferentes países. As organizações internacionais, como a Interpol, deveriam dar mais atenção a este aspecto".[14]

2.3 OCDE

Precursores como a OCDE (Organização para a Cooperação e Desenvolvimento Econômico) ainda em 1982 decidiram por nomear uma comissão de peritos para discutir a cibercriminalidade e a necessidade de mudança nos Códigos Penais[15].

A OCDE é uma organização internacional com sede em Paris, na França, e é composta por 35 países membros que reúnem as maiores economias do mundo, entre eles países emergentes como Chile, México, Turquia e Coréia do Sul. Esses países se reúnem para trocar informações e alinhar políticas com o objetivo de potencializar seu crescimento econômico e colaborar com o desenvolvimento de todos os demais países membros. E foi por meio dessa cooperação que a OCDE tornou-se uma fonte importante de soluções para políticas públicas em um mundo globalizado[16].

2.4 G8

Os G8, grupo internacional que reúne os sete países (EUA, Japão, Alemanha, Reino Unido, França, Itália e o Canadá) mais industrializados e desenvolvidos economicamente do mundo, mais a Rússia, criaram em 1998, um grupo de especialistas para atuar no combate ao crime organizado transnacional, com o objetivo principal de assegurar que nenhum criminoso recebesse refúgio em qualquer lugar do mundo[17]. Foi nessa reunião, no final dos anos 90, que surgiu na cidade de Lyon, na França, o termo cibercrime. O "Grupo de Lyon" utilizou o termo para informar, amplamente, as formas de crimes cometidos por meio da internet, tendo essa reunião sido utilizada exatamente para estipular as maneiras e os métodos utilizados para combater práticas ilícitas na internet[18].

---

[14] NETO, Arnaldo. **Cibercrime e Cooperação Penal Internacional: Um Enfoque à Luz da Convenção de Budapeste,** p. 121. Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/arnaldo-sobrinho-cibercrime-e-cooperacao-penal-internacional.pdf >. Acesso em 30 abr. 2020.

[15] NETO, Arnaldo**. Cibercrime e Cooperação Penal Internacional: Um Enfoque à Luz da Convenção de Budapeste.** Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/arnaldo-sobrinho-cibercrime-e-cooperacao-penal-internacional.pdf >. Acesso em 30 abr. 2020.

[16] BRASIL. Ministério da Economia. **Organização para a Cooperação e Desenvolvimento Econômico – OCDE.** Disponível em: http://www.fazenda.gov.br/assuntos/atuacao-internacional/cooperacao-internacional/ocde>. Acesso em: 08 maio 2020.

[17] NETO, Arnaldo. **Cibercrime e Cooperação Penal Internacional: Um Enfoque à Luz da Convenção de Budapeste**, p. 121. Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/arnaldo-sobrinho-cibercrime-e-cooperacao-penal-internacional.pdf >. Acesso em 30 abr. 2020.

[18] NASCIMENTO, SAMIR. **Cibercrime conceitos, modalidades e aspectos jurídicos-penais.** Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 07 maio 2020

2.5 CONVENÇÃO DE BUDAPESTE

Surge em 2001, em Budapeste, na Hungria, a Convenção sobre Cibercrimes, também conhecida como Convenção de Budapeste, a qual está em vigor desde 2004 e passou a vigorar em 2006 com o Protocolo Adicional à Convenção de Budapeste[19] que criminaliza também condutas racistas ou xenófobas praticadas na rede mundial de computadores.

Ela foi assinada por países do Conselho da Europa e também por não membros e, atualmente já são mais de 67 países que, durante esses anos, foram aderindo a Convenção. Há países signatários que assinaram a Convenção mas que nunca chegaram a ratifica-la; é o caso, por exemplo, da Irlanda, da Suécia e da África do Sul.

A seguir, segue tabela elaborada com base na ETS nº 185 do Conselho da Europa.[20]

TABELA 01

CONSELHO DA EUROPA:	**SIGNATÁRIO**	**RATIFICAÇÃO**	**ENTROU EM VIGOR**
ALBÂNIA	23/11/2001	20/06/2002	01/07/2004
ANDORRA	23/04/2013	16/11/2016	01/03/2017
ARMÊNIA	23/11/2001	12/10/2006	01/02/2007
ÁUSTRIA	23/11/2001	13/06/2012	01/10/2012
ALEMANHA	23/11/2001	09/03/2009	01/07/2009
AZERBAIJÃO	30/06/2008	15/03/2010	01/07/2010
BÉLGICA	23/11/2001	20/08/2012	01/12/2012
BÓSNIA E HERZEGOVINA	09/02/2005	19/05/2006	01/09/2006
BULGÁRIA	23/11/2001	07/04/2005	01/08/2005
CROÁCIA	23/11/2001	17/10/2002	01/07/2004
CHIPRE	23/11/2001	19/01/2005	01/05/2005
DINAMARCA	22/4/2003	21/06/2005	01/10/2005
ESPANHA	23/11/2001	03/06/2010	01/10/2010
ESTÔNIA	23/11/2001	12/05/2003	01/07/2004
ESLOVÊNIA	24/7/2002	08/09/2004	01/1/2005
ESLOVÁQUIA	04/02/2005	08/01/2008	01/5/2008
FINLÂNDIA	23/11/2001	24/05/2007	01/09/2007
FRANÇA	23/11/2001	10/01/2006	01/05/2006
GEÓRGIA	01/04/2008	06/06/2012	01/10/2012
GRÉCIA	23/11/2001	25/01/2017	01/05/2017
HUNGRIA	23/11/2001	04/12/2003	01/07/2004
ISLÂNDIA	23/11/2001	29/01/2007	01/05/2007

[19] CONSELHO DA EUROPA. **Convenção sobre o Cibercrime - ETS nº 189.** Disponível em <https://rm.coe.int/16802ed8cd>. Acesso em 04 maio 2020.
[20] CONSELHO DA EUROPA. **Quadro de assinaturas e ratificações do Tratado - ETS nº 185 – Convenção sobre Cibercrimes.** Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>. Acesso em 24 jun. 2020.

IRLANDA	28/02/2002		
ITÁLIA	23/11/2001	05/06/2008	01/10/2008
LETÔNIA	05/05/2004	14/02/2007	01/06/2007
LIECHTENSTEIN	17/11/2008	27/01/2016	01/05/2016
LITUÂNIA	23/6/2003	18/03/2004	01/07/2004
LUXEMBURGO	28/1/2003	16/10/2014	01/02/2015
MALTA	17/1/2002	12/04/2012	01/08/2012
MOLDÁVIA	23/11/2001	12/05/2009	01/09/2009
MÔNACO	02/05/2013	17/03/2017	01/07/2017
MONTENEGRO	07/04/2005	03/03/2010	01/7/2010
PAÍSES BAIXOS	23/11/2001	16/11/2006	01/03/2007
NORUEGA	23/11/2001	30/06/2006	01/10/2006
NORTE DA MACEDÔNIA	23/11/2001	15/09/2004	01/01/2005
POLÔNIA	23/11/2001	20/02/2015	01/06/2015
PORTUGAL	23/11/2001	24/03/2010	1/7/2010
REPÚBLICA THECA	9/2/2005	22/08/2013	1/12/2013
ROMÊNIA	23/11/2001	12/05/2004	1/9/2004
RÚSSIA			
REINO UNIDO	23/11/2001	25/05/2011	1/9/2011
SAN MARINO	17/03/2017	08/03/2019	01/07/2019
SÉRVIA	7/4/2005	14/04/2009	1/8/2009
SUÉCIA	23/11/2001		
SUÍÇA	23/11/2001	21/09/2011	1/1/2012
UCRÂNIA	23/11/2001	10/03/2006	1/7/2006
TURQUIA	10/11/2010	29/09/2014	01/01/2015

TABELA 02:

NÃO MEMBROS	**SIGNATÁRIO**	**RATIFICAÇÃO**	**ENTROU EM VIGOR**
ÁFRICA DO SUL	23/11/2001		
ARGENTINA		05/06/2018	01/10/2018
AUSTRÁLIA		30/11/2012 a	01/03/2013
CANADÁ	23/11/2001	08/07/2015	01/11/2015
CABO VERDE		19/06/2018	01/10/2018
CHILE		20/04/2017	01/08/2017
COLÔMBIA		16/03/2020	01/07/2020
COSTA RICA		22/09/2017	01/01/2018
ESTADO UNIDOS	23/11/2001	29/09/2006	01/01/2007
FILIPINAS	28/03/2018	01/07/2018	
GANA		0312/2018	01/04/2019
ILHAS MAURÍCIO		15/11/2013	01/03/2014
ISRAEL		09/05/2016	01/09/2016
JAPÃO	23/11/2001	03/07/2012	01/11/2012
MÉXICO			
MARROCOS		29/06/2018	01/10/2018
PANAMÁ		05/03/2014	01/07/2014
PARAGUAI		30/07/2018	01/11/2018
PERU		26/08/2019	01/12/2019

REPÚBLICA DOMINICANA		07/02/2013	01/06/2013
SENEGAL		16/12/2016	01/04/2017
SRI LANKA		29/05/2015	01/09/2015
TONGA		09/05/2017	01/09/2017

A Convenção de Budapeste buscou articular maneiras rápidas e eficazes para lidar com as ameaças presentes no ciberespaço, utilizando-se da cooperação internacional penal. Já em seu preâmbulo se mostra bastante completa e complexa, explicitando palavras como: união, cooperação internacional, equilíbrio, aplicação da lei e os direitos fundamentais, dentro outros. A Convenção traz conceitos e terminologias para que não haja dúvidas quanto à sua aplicação, se mostrando um instrumento jurídico pleno e eficaz de combate à criminalidade cibernética.

Essa Convenção foi o primeiro tratado internacional que buscou abordar a cibercriminalidade e harmonizar as legislações nacionais para que houvesse uma regulamentação supranacional. Pois, não há como se falar em cibercrimes sem que haja uma cooperação internacional, uma verdadeira cooperação entre nações.

Desde sua criação diversos países que não integram o Conselho da Europa[21] aderiram a Convenção, exatamente pelo seu teor ser de interesse de todos. Os signatários incluem países como: Canadá, Chile, Japão, Estados Unidos, Austrália, Argentina, Paraguai e República Dominicana. Podemos perceber que a Convenção sobre Cibercrimes não distingue raça, cultura ou localização geográfica, pois, foi objeto de adesão tanto por países orientais, como ocidentais, por países latino-americanos e pelo sul-europeu.

O preâmbulo da Convenção se mostra preocupado com o risco da rede informática e que informações eletrônicas sejam utilizadas para o cometimento de infrações criminais. Afirma, também, a necessidade de cooperação internacional entre os Estados e a indústria privada no combate a cibercriminalidade, além de uma cooperação rápida, eficaz e confiável, pois, a internet é global e as provas de tais infrações ficam armazenadas e são transmitidas pelas redes.

Além de prezar pelo equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano, a Convenção de Budapeste evoca diversas outras Convenções, como a de Proteção pelos Direitos do Homem e das Liberdades Fundamentais, do Conselho da Europa, de 1950; e o Pacto Internacional sobre Direitos Civis e Políticos, da ONU, de

[21] CONSELHO DA EUROPA. **Convenção sobre o Cibercrime - ETS nº 185**. Disponível em < https://www.migliorisiabogados.com/que-paises-firmaron-y-ratificaron-la-convencion-mundial-contra-el-cibercrimen-budapest-2001/?lang=pt>. Acesso em 04 maio 2020.

1966. Exemplos esses que, reafirmam o direito à liberdade de opinião sem interferência na liberdade de expressão.[22]

Ao final do preâmbulo saúda os recentes movimentos, à época, de cooperação no combate à cibercriminalidade no ciberespaço através de ações empreendidas pelas Nações Unidas, pela OCDE, Pela União Europeia e pelo G8, aproximando legislações penais nacionais e permitindo a utilização de meios de investigação eficazes em matéria de crimes informáticos.

Traz conceitos como, "sistema informático", "dados informáticos", "fornecedor de serviços" e "dados de tráfego". Há um capítulo dedicado ao direito penal que trata de assuntos como: acesso ilegítimo, interceptação ilegítima, interferência de dados, interferência de sistemas, uso abusivo de dispositivos, falsidade informática, e até casos de tentativa ou de cúmplice. Além disso possui um capítulo em específico para tratar da pornografia infantil, trazendo conceitos e condutas que venham a ser praticadas. A Convenção conceitua, ainda, a responsabilidade de pessoas coletivas nas redes, sanções e medidas aplicáveis.

Depois de a seção 1 tratar sobre direito penal, a seção 2 trata amplamente sobre direito processual, endereçando desde processos de busca e apreensão de dados informáticos e interceptação de dados relativos ao conteúdo ou dados de tráfego até competências e princípios de cooperação internacional, extradição e auxílio mútuo. A Convenção sobre o Cibercrime, por ser um tratado do Conselho da Europa, diferentemente da União Europeia, aceita que países do mundo inteiro venham a aderir a Convenção.

Mesmo não sendo membro, o Brasil pode participar de reuniões, atuando de forma seletiva em Comitês que são do seu interesse e que lhe servem como fonte de informações e local para a divulgação de posicionamentos. Vale lembrar que os comitês e grupos de trabalho dos quais o Brasil participa têm levado a convergências políticas em diversas áreas, desde combate à corrupção, até padrões de conduta de multinacionais, políticas de concorrência e fomento ao investimento estrangeiro.[23]

2.6 O BRASIL E A COOPERAÇÃO INTERNACIONAL

O Brasil ainda não aderiu à Convenção de Budapeste. Recentemente, no dia 11 de Dezembro de 2019 foi publicada uma nota no site do Ministério das Relações Exteriores dizendo que "o Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir à Convenção sobre Crimes

---

[22] **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em 13 mar. 2020.

[23] BRASIL. Ministério da Economia. **Organização para a Cooperação e Desenvolvimento Econômico – OCDE.** Disponível em: http://www.fazenda.gov.br/assuntos/atuacao-internacional/cooperacao-internacional/ocde>. Acesso em: 08 maio 2020.

Cibernéticos, também conhecida como Convenção de Budapeste, celebrada em 2001. O processo foi iniciado em julho último, quando o Governo brasileiro manifestou sua intenção de aderir ao instrumento internacional."[24]

O Brasil já pode participar como observador das reuniões sobre a Convenção e seus protocolos. Na própria nota resta claro e evidente que a Convenção só viria a somar à Lei 12.965/2014, o famoso Marco Civil da Internet, além de proporcionar às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, e uma cooperação jurídica internacional voltada à persecução penal dos crimes cibernéticos.

Os cibercrimes, além de resultarem em consequências penais geram também prejuízos econômicos. É o que relata o presidente da ARME, Agência Reguladora Multisetorial da Economia, de Cabo Verde. Ele diz haver um aumento exponencial a nível mundial dos crimes cibernéticos e que Cabo Verde não se diferencia. Alega que em 2015 o mundo perdeu cerca de três trilhões de dólares com problemas de cibersegurança e cibercrime e complementa dizendo que em 2021 a perda é estimulada em seis trilhões de dólares.[25]

Com base nisso e observando as dimensões extraterritoriais que o crime cibernético tem alcançado, o Conselho da Europa em um Fórum sobre Cibercrimes ocorrido em abril de 2019 em Cabo Verde, encorajou os países da CPLP (Comunidade dos Países de Língua Portuguesa) a integrarem a Convenção de Budapeste. Países como: Angola, Brasil, Guiné Bissau, Guiné Equatorial, Moçambique, São Tomé e Príncipe e Timor Leste.[26]

O Brasil ocupa a 70ª posição no índice de segurança cibernética da UIT (União Internacional de Telecomunicações), órgão da Organização das Nações Unidas - ONU. É o segundo país no mundo a sofrer com perdas econômicas advindas de ataques cibernéticos. Segundo os dados mais recentes da UIT entre 2017 e 2018 os prejuízos ultrapassaram os vinte bilhões de dólares. Especialistas calculam que, ainda em 2020, o mercado de segurança cibernética acarretará um prejuízo de cento e cinquenta e um bilhões de dólares.[27]

Há muito a trilhar nesse sentido, principalmente ao se tratar de segurança cibernética. Em 2018 foi publicado o Decreto 9.637 que trata sobre a Estratégia Nacional de Segurança da Informação,

---

[24] BRASIL. Ministério das Relações Exteriores. **PROCESSO de adesão à Convenção de Budapeste – Nota 309**. Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em: 04 maio 2020

[25] ALMEIDA, Sara. INFORPRESS. **Crimes cibernéticos têm aumentado exponencialmente a nível mundial e Cabo Verde não foge à regra – PCA da ARME.** Disponível em: https://expressodasilhas.cv/pais/2020/02/12/crimes-ciberneticos-tem-aumentado-exponencialmente-a-nivel-mundial-e-cabo-verde-nao-foge-a-regra-pca-da-arme/67934>. Acesso em: 08 maio 2020.

[26] AGUIRRE, Lauriane. **Cibercrime como pauta da CPLP.** Disponível em: < https://ceiri.news/cibercrime-como-pauta-da-cplp/>. Acesso em 08 maio 2020.

[27] BRASIL. Senado Notícias. **Brasil é o 2º no mundo em perdas por ataques cibernéticos, aponta audiência.** Disponível em: < https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>. Acesso em 08 maio 2020.

devendo conter ações estratégicas e objetivos relacionados à segurança da informação em consonância com as políticas públicas e os programas do Governo Federal, no inciso I de seu artigo 6º, traz à segurança cibernética.

Dois anos depois, no ano de 2020, é aprovada a Estratégia Nacional de Segurança Cibernética, ou a E-Ciber, por meio do Decreto 10.222 de 05 de fevereiro de 2020. Ela funciona mais como um documento orientador de políticas públicas no âmbito do Poder Executivo, um aprimoramento do arcabouço legal sobre Segurança Cibernética.

Após a edição do decreto da E-Ciber, o Senado se preocupa com a responsabilidade dos entes federativos quanto à segurança cibernética dos serviços públicos brasileiros. A proposta de emenda à Constituição nº 61/2015, do **senador Eduardo Gomes** é de alterar os artigos 22, 23 e 24 da Constituição Federal. Com essa PEC é possível dar à União a prerrogativa de legislar não só sobre a defesa territorial, aeroespacial, marítima e civil, como já faz, mas também sobre a defesa cibernética.[28]

O Supremo, recentemente, já tem lidado com questões técnicas e jurídicas em relação à efetividade de tratados internacionais para a obtenção e a interceptação do conteúdo de comunicações eletrônicas, como as conversas via WhatsApp. Também estão em debate os limites da soberania nacional dos países envolvidos, os critérios de alcance da jurisdição brasileira sobre comunicações eletrônicas e os parâmetros de territorialidade, dentre outros aspectos.[29]

Para o ex-ministro da Justiça e da Segurança Pública, Sérgio Moro, não há razão para que os tribunais brasileiros abram mão de sua soberania e de sua jurisdição sobre crimes praticados no Brasil. Restam dúvidas, portanto, em como investigar e punir provedores de aplicações sem representação no País, como o Telegram. Hoje em dia é necessário um pedido de cooperação internacional para promover investigações envolvendo esse tipo de provedores.[30]

O Ministério Público Federal, juntamente com o Ministério da Justiça e o Ministério das Relações Exteriores são órgãos importantes na atuação e combate ao cibercrime e na cooperação internacional. Representantes do Ministério Público defendem a adesão do Brasil à Convenção de Budapeste e[31] ressaltam ser essencial a cooperação internacional no combate aos crimes

---

[28] LUCA, Cristina de. **Proposta de emenda constituinal diferencia segurança e defesa cibernética.** Disponível em: < https://porta23.blogosfera.uol.com.br/2020/02/16/proposta-de-emenda-constitucional-diferencia-seguranca-e-defesa-cibernetica/>. Acesso em: 12 maio 2020.

[29] LUCA, Cristina de. **Proposta de emenda constituinal diferencia segurança e defesa cibernética.** Disponível em: < https://porta23.blogosfera.uol.com.br/2020/02/16/proposta-de-emenda-constitucional-diferencia-seguranca-e-defesa-cibernetica/>. Acesso em: 12 maio 2020.

[30] HAJE, Lara. **Ministério Público pede rejeição de projeto que proíbe bloqueio do Whatsaap – Representantes do MP, de delegados e peritos defendem adesão do Brasil à Convenção de Budapeste sobre crimes cibernéticos.** Disponível em: <https://www.camara.leg.br/noticias/571408-ministerio-publico-pede-rejeicao-de-projeto-que-proibe-bloqueio-do-whatsapp/>. Acesso em: 12 maio 2020.

[31] HAJE, Lara. **Ministério Público pede rejeição de projeto que proíbe bloqueio do Whatsaap – Representantes do MP, de delegados e peritos defendem adesão do Brasil à Convenção de Budapeste sobre**

cibernéticos.[32] Destacam ainda, que a quantidade de ações envolvendo pornografia infanto-juvenil (2.169) supera as de racismo e de outros crimes de ódio (442).[33]

O Brasil, segundo reportagem, está em oitavo lugar quando se trata de vítimas de ataques de *bankers*, os quais roubam dados bancários de vítimas. No primeiro trimestre de 2020 esse número cresceu 2,5 vezes mais se comparados com o trimestre anterior. Entre os países com maior número de ataques de *malware* bancário, ou *bankers*, estão o Japão, a Espanha, a Itália e o Brasil.[34]

Portanto compreende-se a importância da cooperação internacional não só sob o aspecto político internacional, mas também sob o aspecto econômico, já que diversos países e empresas, para manterem relações com o Brasil, preocupam-se com a higidez e a segurança proporcionada pelo sistema jurídico nacional no combate ao cibercrime.

3 CRONOLOGIA LEGISLATIVA E AS LACUNAS RELACIONADAS AOS CIBERCRIMES

3.1 PROJETO DE LEI 84/1999

No Brasil, o primeiro projeto de lei a tratar sobre o tema foi o projeto 84/1999, que, anos depois, após diversas mudanças, ficou popularmente conhecido como Lei Azeredo. Ele foi proposto pelo deputado Luiz Piauhylino, em 1999, cujo objetivo era definir crimes cibernéticos. Em 2003, o projeto foi aprovado pela Câmara, mas foi em 2008, em sua versão final, que o Senador Eduardo Azeredo enviou um texto mais abrangente, porém, pela quantidade de brechas e dualidades de pontos controversos, o texto não conseguia ser aprovado.

Esse projeto visava criminalizar doze tipos de ações praticadas na internet, tornando-as passíveis de prisão e multa, seriam elas: acessar um sistema informatizado sem autorização; obter, transferir ou fornecer dados ou informações sem autorização; divulgar ou utilizar de maneira indevida informações e dados pessoais contidos em sistema informatizado; destruir, inutilizar ou deteriorar coisas alheias ou dados eletrônicos de terceiros; inserir ou difundir código malicioso em sistema informatizado; inserir ou difundir código malicioso seguido de dano; estelionato eletrônico; atentar

---

crimes cibernéticos. Disponível em: <https://www.camara.leg.br/noticias/571408-ministerio-publico-pede-rejeicao-de-projeto-que-proibe-bloqueio-do-whatsapp/>. Acesso em: 12 maio 2020.

[32]BRASIL. Ministério Público Federal. **Fortalecer a cooperação internacional é essencial para enfrentar crimes cibernéticos, defende MPF.** Disponível em: < http://www.mpf.mp.br/pgr/noticias-pgr/fortalecer-a-cooperacao-internacional-e-essencial-para-enfrentar-crimes-ciberneticos-defende-mpf>. Acesso em: 12 maio 2020.

[33] In: Brasília de Fato. **Crimes cibernéticos levam MPF a atuar em 2.611 processos em 2018.** Disponível em: <https://brasiliadefato.com.br/politica-e-brasil/2019/02/crimes-ciberneticos-levam-mpf-a-atuar-em-2-611-processos-em-2018/>. Acesso em: 12 maio 2020.

[34] FABRO, Clara. **Golpe de roubo de dados bancários cresce e Brasil é um dos mais afetados.** Disponível em: < https://www.techtudo.com.br/noticias/2020/05/golpe-de-roubo-de-dados-bancarios-cresce-e-brasil-e-um-dos-mais-afetados.ghtml>. Acesso em 01 jun. 2020.

contra a segurança de serviço de utilidade pública; interromper ou perturbar serviço telegráfico, telefônico, informático, telemático ou sistema informatizado; falsificar dados eletrônicos ou documentos públicos; falsificar dados eletrônicos ou documentos particulares e discriminar raça ou cor por meio da rede de computadores.[35]

Inicialmente o projeto era considerado muito amplo e rígido. Além disso, a proposta chegou a ser chamada de "AI-5 Digital", em uma referência ao ato que reduziu liberdades individuais durante a ditadura militar. Pelo texto inicial, seria crime a gravação de um CD com arquivos que infringem as leis de direitos autorais.

Devido à sua rigidez o projeto de lei 84/1999 ficou anos adormecido. Em 2008 a discussão foi retomada por Azeredo, porém, pela grande quantidade de brechas e pontos dúbios, o projeto passou mais alguns anos em debate. Até que em 2011 o projeto passa por algumas mudanças em seu texto, onde dos vinte e três artigos originais, dezessete deles foram retirados, ou seja, apenas seis artigos foram mantidos fazendo com que surgisse assim, a Lei 12.735/2012[36].

3.2 Lei 12.735/2012 - AZEREDO

A Lei 12.735/2012, derivada do projeto de lei Azeredo de 1999, mesmo sendo reescrita e seus pontos polêmicos rejeitados quase que em sua totalidade, manteve em aberto alguns pontos necessários, como punir quem invade computadores, derruba redes e sites, além de divulgar informações sigilosas. A lei foi complementada pela Lei 12.737/2012, mais conhecida como Lei Carolina Dieckmann, que, entretanto, ainda manteve o tema complexo e repleto de lacunas.

A lei 12.735/2012 buscou determinar a criação de setores e equipes especializadas no combate aos delitos praticados na internet. Vale dizer que mesmo após alguns anos de sancionamento da lei

---

[35] LANDIM, Wikerson. **Conheça a Lei Azeredo, o SOPA brasileiro.** Disponível em: <https://www.tecmundo.com.br/ciencia/18357-conheca-a-lei-azeredo-o-sopa-brasileiro.htm>. Acesso em: 10 maio 2020.

[36] BRASIL. **Lei 12.735, de 30 nov. 2012. Tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em 03 mar 2020.

12.735/2012 grande parte dos Estados não criaram delegacias e setores especializados na repressão de crimes informáticos, muitos por não possuírem conhecimento na área ou quando detinham eram desprovidos de estrutura física e pessoal capacitado. Além de que a criação de delegacias especializadas em crimes informáticos gera um considerável aumento de ocorrências em apenas um local, pois não há um filtro no encaminhamento das ocorrências por parte das outras delegacias. Sugere-se que as delegacias especializadas lidem apenas com crimes próprios e de maior complexidade, deixando as demais ocorrências para o atendimento de cada circunscrição. [37]

No mesmo dia que entrou em vigor a Lei 12.735, derivada do projeto de lei Azeredo, foi o dia em que entrou em vigor a Lei 12.737/2012, intitulada de Lei Carolina Dieckmann, que também buscou tipificar crimes. Ou seja, o projeto de lei nº 2.793/2011[38] que deu início a Lei Dieckmann, a qual foi criada três meses depois do projeto de lei nº 2.126/2011[39], que futuramente se transformaria no Marco Civil da Internet, tramitou na Câmara por apenas 172 dias[40] e já foi para o Senado, um verdadeiro recorde, enquanto o projeto de lei 2.126/2011 só viria a entrar em vigor três anos depois dando início ao Marco Civil da Internet.

Ou seja, os temas ciberespaço, cibercrime, segurança cibernética, entre outros, ficaram adormecidos nas pautas do legislativo e do executivo por anos, por não dizer, por uma década. Pois, vale lembrar que o Projeto de Lei 84 surgiu em 1999, retomado por Azeredo em 2008, mas diversos projetos de lei sobre o tema só foram surgir em meados de 2011.

3.3 Lei 11.829/2008 – PEDOFILIA NA INTERNET

Para não dizer que não houve muitos avanços na legislação cibernética nesses dez anos pode-se ressaltar a Lei 11.829/2008,[41] que aprimora o combate à produção, venda e distribuição de pornografia infantil, bem como criminaliza a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet, alterando assim o Estatuto da Criança e do Adolescente.

Segundo o texto legal, as páginas com conteúdo adulto inadequado a crianças e adolescentes

---

[37] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

[38] BRASIL. **Projeto de Lei nº 2.793, de 29 nov 2011. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.** Disponível em: < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em 19 maio 2020.

[39] BRASIL. **Projeto de Lei nº 2.126, de 24 ago 2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em 19 maio 2020.

[40] VENTURA. Felipe. **Dieckmann X Azeredo: como se comparam os dois projetos de lei para crimes virtuais**. Disponível em: < https://gizmodo.uol.com.br/projeto-leis-dieckmann-azeredo/>. Acesso em: 18 maio 2020.

[41] BRASIL. **Lei 11.829, de 25 nov 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 25 maio 2020.

estariam obrigadas, sob pena de multa, avisarem sobre a natureza de seu conteúdo, a usarem código que limite o acesso de crianças e adolescentes, a exigirem identificação válida para o acesso, e a manterem os registros de acesso por três meses. A redação também impedia que sites de acesso irrestrito contivessem "ilustrações, imagens, propaganda, legendas ou textos que façam apologia de bebidas alcoólicas, tabaco, drogas ilegais, armas ou munições.[42]

3.4 Lei 12.737/2012 - CAROLINA DIECKMANN

O projeto de lei 2.793/2011, posteriormente transformado na Lei Ordinária 12.737[43], mais conhecida como Lei Carolina Dieckmann, em razão de a atriz ter sido vítima de crime cibernético por ter seu computador invadido e suas imagens furtadas, divulgadas e utilizadas para à pratica de extorsão, altera também o Código Penal[44] e dispõe sobre a tipificação criminal de delitos informáticos. Surgiu como uma alternativa a Lei Azeredo que com o tempo se tornou inofensiva e ambas passaram a se complementar.

Na prática a Lei Dieckmann buscou restaurar vários pontos polêmicos que a Lei Azeredo perdeu, sendo a primeira lei brasileira criada exclusivamente para a tipificação de crimes cibernéticos. Representou grandes avanços no combate aos crimes digitais ao tipificar um novo crime, o qual altera o Código Penal e inclui o artigo 154-A, que se trata sobre a invasão de dispositivo informático.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades.

O primeiro questionamento é se seria necessário que o indivíduo violasse de alguma forma o dispositivo, logo, ele deveria estar condicionado a uma barreira de segurança para que se valha da invasão. Além de que mesmo violado o dispositivo de segurança não seria considerado crime o acesso indevido, sem interesse em obter, adulterar, entre outros. Outra crítica feita à lei foi quanto ao uso do termo "dispositivo informático" ao invés de "dispositivo eletrônico" o qual abrangeria em sua totalidade todos os aparelhos que possuem acesso à internet, sejam eles celulares, smartphones,

---

[42] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

[43] BRASIL. **Lei 12.737, de 30 nov. 2012. Dispõe sobre a tipificação criminal de delitos informáticos**; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 12. out. 2019

[44] BRASIL. **Código Penal - Decreto-Lei 2.848, de 07 dez. 1940.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em 12 out. 2019.

televisores, dentre outros.[45]

De certa maneira, alguns problemas não se relacionavam à falta de legislação, pois, diversos crimes já eram previstos no Código Penal, sendo a Internet apenas um meio alternativo de cometê-los, os chamados crimes impróprios. Em outros casos, no entanto, a dificuldade estava em enquadrar a conduta criminosa ao fato por falta de previsão legislativa. No caso Carolina Dieckmann por não haver à época dispositivo prevendo delitos informáticos e nem todas as ações praticadas estarem previstas no Código Penal, não puderam todas as ações serem punidas por falta de previsão legal, devendo utilizar-se, na medida do possível, de analogias.

Até o advento desta lei não havia dispositivo legal que efetivamente tipificasse a invasão de dispositivo informático, restando apenas a impunidade. Foi com a edição do artigo 154-A do Código Penal e de seus parágrafos, que foi possível a previsão de punição de quem invade dispositivo, onde o primeiro parágrafo equipara o sujeito que produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o objetivo de praticar as condutas previstas no caput do artigo.

No parágrafo segundo aumentou a pena de um sexto à um terço se a invasão resultar em prejuízo econômico ou de um terço a metade se praticado contra Presidente da República, Governador, Prefeito, Presidente do STF, Presidente da Câmara, do Senado, dentre outros, como no parágrafo quinto[46]

Além do crime de invasão de dispositivo informático, a lei 12.737/2012 alterou o artigo 266 do Código Penal, incluindo em seu parágrafo primeiro não só a interrupção e perturbação de serviços telegráficos e telefônicos, os serviços informáticos, telemáticos e de informação de utilidade pública. Esse tipo de crime é bem comum, visando inutilizar ou reduzir a capacidade de algum serviço disponibilizado na internet, com o objetivo de causar transtornos e consequentemente gerar prejuízos ao provedor e utilizadores do serviço.[47] Por fim, incluiu no rol de falsificação de documentos particulares no artigo 298, parágrafo único, do Código Penal equiparando a documento pessoal a falsificação de cartão de crédito ou débito.

Ou seja, a Lei 12.737/2012 foi muito importante, pois, por meio do artigo 154-A do Código

---

[45] NASCIMENTO, Samir de Paula. **Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais.** Disponível em: < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em: 18 maio 2020.

[46] BRASIL. **Lei nº 12.737, de 30 nov 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 19 maio 2020.

[47] BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012.** Disponível em: < https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>. Acesso em 19 maio 2020.

Penal criou um novo tipo penal, a invasão de dispositivo informático, além de alterar o artigo 266, do referido código, incluindo a interrupção não só telegráfica e telefônica, como também, a interrupção informática, telemática e de informação de utilidade pública. Por fim, incluiu o parágrafo único do artigo 298, também do Código Penal, para equiparar o cartão de crédito e de débito a documento pessoal.

Logo, com o advento da lei, quem pratica o delito de invadir o computador ou dispositivo informático alheio com objetivo de conseguir, alterar ou destruir dados sem autorização, pode ser condenado. O mesmo vale para tentativas derrubar sites, interromper serviços, *hackear* servidores, além de cometer delitos pela internet como a falsificação de documentos ou até mesmo cartões de bancos e etc. Porém muitos crimes praticados na internet ainda não possuem legislação específica e há uma certa dificuldade por parte dos agentes do Estado em detectá-los e puni-los. É possível perceber o quão frágil e polêmico é o assunto sobre cibercrimes no Brasil e no mundo.

3.5 MARCO CIVIL DA INTERNET

O projeto de lei foi elaborado com base no documento "Princípios para a governança e o uso da internet", do Comitê Gestor da Internet no Brasil, organismo multissetorial responsável por integrar iniciativas de uso e desenvolvimento da internet brasileira. O documento é resultado de uma consulta pública promovida entre 2009 e 2010, na qual foram arroladas mais de 800 contribuições de diferentes representantes da sociedade civil. Entre os principais eixos temáticos a privacidade, a neutralidade da rede e a inimputabilidade de rede.[48]

Paulo Rená explicita, em sua dissertação de mestrado, que é incoerente a proposta de uma norma penal antes mesmo da existência de uma legislação civil. Uma norma que pudesse disciplinar de forma específica os direitos referentes ao uso da Internet no Brasil e, posteriormente, a regulação da rede. Porém, no Legislativo, a urgência se dava em cima da criminalização de atos praticados na Internet, antes mesmo que fosse possível saber com clareza quais condutas poderiam ou não ser praticadas no ambiente cibernético.[49]

Por esse motivo, outro projeto de lei importante para a legislação brasileira, não só no âmbito penal mas também no âmbito civil, foi o Projeto de Lei 2.126/2011 que se transformou na Lei

---

[48] BEZERRA, Arthur; WALTZ, Igor. **Privacidade, Neutralidade e Inimputabilidade da Internet no Brasil: avanços e deficiências no projeto do Marco Civil.** In: Revista Eptic Online, vol. 16, n.2, p.161-175, mai-ago 2014. Disponível em: < https://ridi.ibict.br/bitstream/123456789/858/2/Arthur.pdf>. Acesso em: 25 maio 2020.

[49] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

12.965/2014, mais conhecida como Marco Civil da Internet. O qual é deveras tão importante quanto os dispositivos penais, pois, legislam voltado para direitos e garantias fundamentais e à luz da liberdade de expressão. O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.[50] É possível perceber que o enfoque é o usuário comum da internet, enquanto os demais dispositivos trazem apenas previsões penais.

O Marco Civil, popularmente conhecido como Constituição da Internet Brasileira, é historicamente originário do decálogo de princípios propostos, em 2009, pelo Comitê Gestor da Internet Brasileira, que estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil. O CGI sistematizou dez princípios, foram eles: a) liberdade, privacidade e direitos humanos; b) governança democrática e colaborativa; c) universalidade; d) diversidade; e) inovação; f) neutralidade da rede; g) inimputabilidade da rede; h) funcionalidade, segurança e estabilidade; i) padronização e interoperabilidade; e j) ambiente legal e regulatório.[51]

Um dos objetivos do Marco Civil era de definir os direitos oriundos da utilização da internet, prevendo o que se pode ou não fazer civilmente, antes mesmo que condutas fossem criminalizadas no ambiente cibernético. Exigia-se que a abordagem fosse feita pelo prisma dos direitos dos usuários e que não fossem impostas obrigações excessivas aos provedores.[52]

Paulo Rená defende ainda que o Marco Civil da Internet está articulado em três eixos centrais, o dos direitos, o dos deveres e das atribuições do Poder Público[53]. A lei 12.965/2014 em seu artigo 2º diz que o uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como o reconhecimento da escala mundial da rede, os direitos humanos, o exercício da cidadania em meios digitais, a livre iniciativa, a livre concorrência, a defesa do consumidor, a finalidade social, dentre outros.

Liberdade de expressão essa que é relativizada do ponto de vista da Constituição, que veda expressamente o anonimato ao garantir a liberdade de expressão. No Marco Civil da Internet, adotou-se a premissa de que nem todo uso da Internet envolve uma efetiva expressão ou manifestação de

---

[50] BRASIL. **Lei 12.965, de 23 de abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 25 maio 2020.

[51] NASCIMENTO, SAMIR. **Cibercrime conceitos, modalidades e aspectos jurídicos-penais.** Disponível em: < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 18 maio 2020.

[52] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

[53] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

pensamento, de forma que a mera navegação não requereria a autenticação e identificação dos usuários.[54]

Já no artigo 3º, o Marco Civil da Internet estabelece princípios, como a proteção da privacidade e dos dados pessoais, a preservação e a garantia de neutralidade da rede, a responsabilização dos agentes, entre outros. Essa neutralidade de rede prevista no inciso IV, do artigo 3º faz com que a rede não discrimine o conteúdo para seu carregamento, ou seja, vídeos, áudios, textos e imagens são carregados da mesma forma, sem discriminação.

O artigo 4º promove o direito de acesso à internet a todos e de acesso a informação, algo problemático quando uma pesquisa divulgada recentemente pelo IBGE diz que um a cada quatro brasileiros não possui acesso à Internet, o que equivale a quarenta e seis milhões de pessoas sem internet em suas residências no Brasil.[55] Chega a afirmar em seu artigo 8º, que a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.[56]O capítulo é finalizado com o artigo 5º que traz alguns conceitos como: "internet", "terminal", "endereço de IP", "registro de acesso" e etc.

A Lei inicia o capítulo dois falando sobre direitos e garantias dos usuários, ressaltando novamente a importância do acesso à internet para o exercício da cidadania e assegurando alguns direitos em seus incisos.

No capítulo três trata sobre a neutralidade de rede, a proteção dos registros, dados pessoais e às comunicações privadas. A norma especifica critérios para a guarda de registros de conexão, a guarda de registros de acesso a aplicações de internet na provisão de conexão e a responsabilidade por danos decorrentes de conteúdo gerado por terceiros, além de explicitar a necessidade de requisição judicial para o fornecimento de registros de conexão ou registros de acesso a aplicações de internet. Por último, no capítulo quatro, finaliza o terceiro bloco definido por Renáº[57], tratando sobre a atuação do Poder Público.

---

[54] SANTARÉM, Paulo Renáº da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: < https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 23 maio 2020.

[55] TOKARNIA, Mariana. **Um em cada 4 brasileiros não tem acesso à internet.** Disponível em: < https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/um-em-cada-quatro-brasileiros-nao-tem-acesso-internet>. Acesso em: 25 maio 2020.

[56] BRASIL. **Lei 12.965, de 23 de abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 25 maio 2020.

[57] SANTARÉM, Paulo Renáº da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

Após esse panorama da legislação é possível perceber que alguns dos pontos polêmicos do Marco Civil relacionam-se à guarda de registros de conexão e de uso de serviços, a remoção de conteúdo gerado por terceiros e a liberdade de expressão e o anonimato.[58] O debate sobre a guarda de registros já havia sido amplamente realizado nos projetos de lei que diz respeitam aos cibercrimes, e havia uma grande expectativa sobre como o tema seria tratado.

A legislação prevê em seu artigo 18, que o provedor de conexão não será responsabilizado civilmente diante de danos decorrentes de conteúdo gerado por terceiros. Mas, complementa em seu artigo 19 que, para assegurar a liberdade de expressão e impedir a censura, o provedor de aplicação de internet só será responsabilizado civilmente por danos a terceiros se, após ordem judicial, não tomar as devidas providências dentro do prazo estipulado. Como por exemplo, tornar um conteúdo indisponível.

Ao longo dos debates que precederam a aprovação da Lei foi apresentada a proposta de que o conflito fosse resolvido entre as partes por meio de acordo ou entendimento autônomo, desonerando assim o Poder Judiciário. Porém o modelo não foi socialmente nem internacionalmente aceito, fazendo com que qualquer remoção de conteúdo necessitasse de ordem judicial, trazendo novamente o Poder Judiciário como garantidor da legalidade na oposição ao exercício da liberdade de expressão.[59]

O Marco Civil buscou então democratizar o debate a partir do momento que realizou audiências públicas, pois, nelas encontra o reconhecimento da legitimidade que o debatedor ostenta onde todos possuem igualmente seu lugar de fala e interesses comuns, todos legitimamente cidadãos.

Com o Marco Civil, foi possível vislumbrar na Internet um local de Direito Público fora dos limites do Estado, permitindo uma independência do cidadão em relação ao mesmo. Buscou-se um equilíbrio e uma harmonização entre os direitos fundamentais e o combate ao crime de tal forma que esse combate não violasse direitos e garantias fundamentais, fazendo com que tais direitos fossem ressignificados no âmbito cibernético.

Ou seja, o Marco Civil foi de extrema relevância para um novo conceito de democratização de participação popular no processo legislativo, pois, ao final do processo há um novo sujeito coletivo de direitos, uma nova leitura aos direitos fundamentais e uma experiência de interlocução em um

---

[58] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

[59] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

novo espaço público não estatal.[60]

Além de ser um tema extremamente atual no ano de 2020, pois, no dia vinte e sete de maio deste ano o Supremo Tribunal Federal começou o julgamento da ADPF 403 que trata sobre a suspensão dos serviços de aplicativo de conversas e a ADI 5527 a qual questiona a interpretação de alguns dispositivos do Marco Civil da Internet.

As ações, relatadas pelo ministro Edson Fachin e pela ministra Rosa Weber, respectivamente, foram objeto de audiência pública em 2017, reunindo representantes do WhatsApp, do Facebook, da Polícia Federal e do Ministério Público, além de pesquisadores e especialistas da área informática. A primeira questiona se decisões judiciais podem interromper serviços de mensagens, no caso em questão, do WhatsApp. A segunda questiona os artigos da Lei 12.965/2014, como o parágrafo segundo do artigo 10º e as sanções do artigo 12º.[61]

Em seu voto, onde leva-se em consideração ser constitucional ou não o bloqueio do WhatsApp por meio de decisões judiciais, a ministra Rosa Weber votou por afastar a ideia de que artigos do Marco Civil da Internet venham a ferir o direito de livre comunicação e o princípio da livre iniciativa, ambos previstos na Constituição Federal. Além de destacar que tais artigos não sejam usados por juízes para a suspensão de serviços como o WhatsApp.[62] A votação encontra-se suspensa, por pedido de vista do Ministro Alexandre de Moraes.

O inciso II, do artigo 10º desta lei diz que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º".

Além do artigo 11º da mesma lei que diz que:

> Qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet no território deve respeitar a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos

---

60 SANTARÉM, Paulo Renã da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 25 maio 2020.

61 SIMÕES, Lucas. **Ações sobre WhatsApp e Marco Civil da Internet estão em pauta no STF.** Disponível em < https://www.moneytimes.com.br/acoes-sobre-whatsapp-e-marco-civil-da-internet-estao-na-pauta-do-stf/>. Acesso em: 27 mai 2020

62 GOMES, Helton. **Em voto, Weber afasta uso do Marco Civil da Internet para bloquear WhatsApp.** Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/05/27/em-voto-weber-afasta-uso-do-marco-civil-da-internet-para-bloquear-whatsapp.htm>. Acesso em: 01 jun 2020.

registros".[63]

A Ministra Rosa Weber, do Supremo Tribunal Federal, chega a afirmar que tornar a criptografia algo ilegal seria um retrocesso.[64]

Por fim, a ministra ainda diz que no artigo 12 não há nada na lei que autorize a suspensão de serviços de comunicação. Do seu ponto de vista a lei permite apenas que empresas que descumprem ordens judiciais tenham suspensas suas atividades que envolvam "coleta, armazenamento, guarda e tratamento de registros e dados pessoais ou de comunicação". Para a Ministra isto não quer dizer que a lei autorize que juízes utilizem do Marco Civil da Internet para suspender o acesso a tais aplicações.[65]

3.6 E-CIBER

Outro marco normativo recentemente aprovado e tão importante quanto para a proteção do ciberespaço ocorreu no ano de 2018 com a criação do Decreto nº 9.637[66], que revogou os Decretos 3.505[67], de 13 de junho de 2000, que instituía a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal e o Decreto 8.135[68], de 4 de novembro de 2013, que dispunha sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitações nas contratações que possam comprometer a segurança

---

[63] BRASIL. **Lei 12.965, de 23 de abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 01 jun 2020.

[64] GOMES, Helton. **Em voto, Weber afasta uso do Marco Civil da Internet para bloquear WhatsApp.** Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/05/27/em-voto-weber-afasta-uso-do-marco-civil-da-internet-para-bloquear-whatsapp.htm>. Acesso em: 01 jun 2020.

[65] GOMES, Helton. **Em voto, Weber afasta uso do Marco Civil da Internet para bloquear WhatsApp.** Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/05/27/em-voto-weber-afasta-uso-do-marco-civil-da-internet-para-bloquear-whatsapp.htm>. Acesso em: 01 jun 2020.

[66] BRASIL. **Decreto 9.637, de 26 dez 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em: 27 maio 2020.

[67] BRASIL. **Decreto 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 24 jul. 2020.

[68] BRASIL. Decreto 8.135, de 04 de novembro de 2013. **Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em: 24 jul. 2020.

nacional.

O Decreto 9.637 institui então a Política Nacional de Segurança da Informação, ao prever em seus incisos I e II, do artigo 2º, que para sua implementação a segurança da informação abrange a segurança cibernética e a defesa cibernética.

A Segurança da Informação abrangeria em geral a Segurança Cibernética, a Defesa Cibernética, a Segurança Física e a Proteção de Dados Organizacionais, além de ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Mas, é preciso recuar para entender as diferenças, mas também as semelhanças, existentes entre a segurança e defesa cibernética. Devido as constantes e fortes evoluções tecnológicas, surgiram com o tempo questionamentos sobre até aonde iriam as iniciativas governamentais, os limites de atuação de cada Estado diante o ambiente cibernético e as próprias iniciativas dos Estados em ações próprias de defesa cibernética nacional.

A Defesa Cibernética, como o próprio nome diz remete a uma ideia militar, um tipo de ação tática operacional em virtude de um inimigo ou ameaça iminente. São características da Defesa Cibernética: a defesa, visando conter danos já ocorridos a sistemas e instituições; só é posta em execução em casos específicos de ataques contra infraestruturas críticas e sistemas de governo; por esse motivo, é uma ação essencialmente bélica, realizada pelo Comando de Defesa Cibernética, o qual é subordinado ao Ministério da Defesa, composto por um quadro essencialmente de militares; possui alvo certo e só age após a identificação do agente, com ação limitada no tempo e no espaço.[69]

Já a Segurança Cibernética consiste em ações voltadas para a segurança da informação no espaço cibernético. A Segurança Cibernética: visa a proteção, elevando o nível de resiliência de sistemas e instituições, mas também de proteção à sociedade de maneira geral; seu quadro é composto por analistas do Departamento de Segurança da Informação e Comunicação, do Gabinete de Segurança Institucional da Presidência da República; é uma atividade contínua e rotineira, que compreende ações procedimentais e padronizadas que podem ser utilizadas em diferentes sistemas e organizações; portanto se trata de uma condição, ilimitada no tempo e no espaço; é uma ação planejada no nível político, conduzida no nível estratégico e realizada no nível tático, ou seja, estabelece procedimentos de reestabelecimento de sistema, mas não enseja ataques;[70]

---

[69] SABBAT, Arthur. **Defesa Cibernética e Segurança Cibernética: Diferenças e Semelhanças.** Disponível em < https://www.securityreport.com.br/destaques/defesa-cibernetica-e-seguranca-cibernetica-diferencas-e-semelhancas/#.Xxr2Jm1KjIU> Acesso em: 24 jul.2020.

[70] SABBAT, Arthur. **Defesa Cibernética e Segurança Cibernética: Diferenças e Semelhanças.** Disponível em < https://www.securityreport.com.br/destaques/defesa-cibernetica-e-seguranca-cibernetica-diferencas-e-

Dada a importância do tema, o Gabinete de Segurança Institucional da Presidência da República após 31 reuniões e 7 meses de estudos e debates, com a participação de mais de 40 órgãos e entidades do governo, além de instituições privadas e do setor acadêmico elaboraram a E-Ciber fazendo com que fosse criado no dia 05 de fevereiro de 2020 o Decreto nº 10.222[71], o qual aprova a Estratégia Nacional de Segurança Cibernética.[72]

A medida tem validade de um quadriênio, ou seja, valerá do período concebível entre 2020 e 2023, devendo ser revisada periodicamente. Além de preencher uma importante lacuna no arcabouço normativo nacional sobre segurança cibernética, estabelece ações que buscam modificar de forma cooperativa características que refletem o posicionamento de instituições e indivíduos.

Na primeira parte, o documento faz um diagnóstico atual sobre a situação da segurança cibernética brasileira e em seguida estabelece propostas de ação a serem colocadas em prática. Assim foram estabelecidos os objetivos estratégicos nacionais e as respectivas ações estratégicas. Tais objetivos foram analisados sob sete eixos, são eles: Governança da Segurança Cibernética Nacional; Universo Conectado e Seguro: Prevenção e Mitigação de Ameaças Cibernéticas; Proteção Estratégica; Dimensão Normativa; Pesquisa, Desenvolvimento e Inovação; Dimensão Internacional e Parcerias Estratégicas e a Educação à estrutura dos sete eixos de atuação Estratégica.[73]

A E-Ciber busca nortear as ações estratégicas do país ao tratar da Segurança Cibernética, trazendo diretrizes basilares para o setor público, o setor produtivo e a sociedade em geral, para que todos possam usufruir de um espaço cibernético inclusivo, confiável e seguro.

Assim tem-se buscado ações estratégicas para que tal objetivo seja atingido, como: fortalecer as ações de governança cibernética; estabelecer um modelo centralizado de governança em âmbito nacional; promover um ambiente colaborativo, participativo, confiável e seguro, envolvendo setor público, privado e a sociedade; elevar o nível de proteção do Governo; elevar o nível de proteção das Infraestruturas Críticas Nacionais; aprimorar o arcabouço legal sobre segurança cibernética; ampliar a cooperação internacional do Brasil em segurança cibernética; ampliar a parceria em segurança cibernética entre o setor público, privado e sociedade e, por fim, elevar o nível de maturidade da

semelhancas/#.Xxr2Jm1KjIU> Acesso em: 24 jul.2020.

[71] BRASIL. **Decreto 10.222, de 05 fev 2020. Aprova a Estratégia Nacional de Segurança Cibernética.** Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 27 maio 2020.

[72] BRASIL. Departamento de Segurança da Informação. **E-Ciber.** Disponível em: < http://dsic.planalto.gov.br/links-destaques/e-ciber>. Acesso em: 28 maio 2020.

[73] BRASIL. Departamento de Segurança da Informação. **E-Ciber.** Disponível em: < http://dsic.planalto.gov.br/links-destaques/e-ciber>. Acesso em: 28 maio 2020.

sociedade ao se tratar de segurança cibernética.[74]

Além de propor a realização de fóruns de governança, o estabelecimento de requisitos mínimos de segurança cibernética nas contratações pelos órgãos públicos, a implementação de programas e projetos sobre governança cibernética, além intensificar o combate à pirataria de software, recomendar a adoção de soluções nacionais de criptografia observando a legislação específica, entre outros.[75]

O objetivo disso tudo é tornar o Brasil um país próspero e confiável no ambiente digital como condição ideal para o crescimento econômico e o desenvolvimento social, além de fortalecer o cenário brasileiro em relação a segurança cibernética internacional e diversas formas de lidar com ameaças cibernéticas.

4 COMPATIBILIDADE ENTRE A LEGISLAÇÃO BRASILEIRA ATUAL E A CONVENÇÃO DE BUDAPESTE.

A chegada das redes informatizadas e interligadas mundialmente no século XX e sua rápida propagação e desenvolvimento nos anos que se seguiram, fez com que especialistas se preocupassem cada vez mais com os usuários da internet. Foi um verdadeiro agregador e facilitador na comunicação entre indivíduos pelo mundo todo, trazendo diversas benesses e, com elas, os malefícios da rede.

Com isso, além da necessidade de se preocupar com cibercrimes impróprios, condutas ilícitas já existentes que eram praticadas nesse novo ambiente, foi preciso lidar também com novas condutas, os chamados cibercrimes próprios. A competência e a jurisdição já não eram tão simples em se definir, pois se tratavam de crimes transnacionais.

É nesse cenário que surge no mundo todo a preocupação com os crimes cibernéticos. Foi possível perceber que mais importante que punir delitos, é a necessidade de uma legislação que preveja quais condutas podem ou não ser praticadas, para que só assim pudesse os autores serem enquadrados e julgados por seus atos.

Após o apanhado histórico foi possível perceber quão frágil e inócua é a legislação brasileira. Há no ordenamento jurídico uma série de leis esparsas que buscam tratar sobre diversos temas, onde

---

[74] BRASIL. Departamento de Segurança da Informação. **E-Ciber.** Disponível em: < http://dsic.planalto.gov.br/links-destaques/e-ciber>. Acesso em: 28 maio 2020.

[75] CALIXTO, Larissa. **E-Ciber: governo determina uma série de padrões para segurança cibernética.** Disponível em < https://congressoemfoco.uol.com.br/governo/e-ciber-governo-determina-uma-serie-de-padroes-para-seguranca-cibernetica/?aff_source=56d95533a8284936a374e3a6da3d7996>. Acesso em 28 maio 2020.

não trazem uma conceituação adequada, inexistindo um código específico que consolide taxativamente os crimes cibernéticos. Isto se torna preocupante haja vista o crescimento exponencial de usuários da internet e de sistemas informatizados.

Portanto, a legislação brasileira, tanto civil, como penal, seja ela no âmbito processual ou não, tem muito a crescer e acrescentar dentro do ordenamento jurídico. Por mais que tenham surgido diversos movimentos e legislações criadas em função do tema ciberespaço, conceitos e terminologias ainda são muito vagos.

Inicialmente a preocupação foi de criar uma legislação que punisse os velhos e novos crimes praticados na internet, fossem eles crimes impróprios ou próprios. Porém, logo se percebeu que seria necessária uma legislação que regulasse condutas, civilmente, antes mesmo que fosse possível puni-las. Em 2014 o Marco Civil da Internet foi um instrumento importante para avanços nessa área, porém, a deficiência legislativa na tipificação de delitos virtuais possui um longo caminho a percorrer.

De fato o vácuo legal cria uma sensação de impunidade. Vale lembrar que o direito penal brasileiro não recepciona analogia *in malam parte* e nem cria novos delitos por meio de decreto. Isto faz com que o processo se torne muito mais complicado, pois torna a vacância legal de crimes próprios infinitamente mais perigosa que a de crimes impróprios. Pois, nesses, por mais que o Código Penal seja de 1940, crimes como fraude, roubo, furto, estelionato, falsificação, falsa identidade dentre outros estão previstos em lei. Já nos crimes próprios a conduta praticada não pode ser objeto de uma ação penal quando não há previsão legal em legislação esparsa alguma.[76]

Uma das ações do século XXI, regulando o ciberespaço, ocorreu em 2008, quando o Estatuto da Criança e do Adolescente sofreu alterações para suprir a necessidade de crimes impróprios, a pedofilia. Crimes esses que estavam sendo praticados em um novo meio, o digital. Essa alteração surgiu por meio da inclusão dos artigos 241-A e 241-B do ECA.[77]

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1o Nas mesmas penas incorre quem:

[76] BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012**. Revista Âmbito Jurídico. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>. Acesso em: 02 jun 2020.

[77] BRASIL**. Lei no 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 09 jun. 2020.

> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Alguns anos depois leis foram criadas buscando esta regulação do ciberespaço. O Marco Civil, buscou estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil. A E-Ciber visou a segurança cibernética e a Lei Carolina Dieckmann foi a primeira a tipificar crimes cibernéticos criando o crime de invasão de dispositivo.

Mas, sendo a previsão legal brasileira direcionada para os cibercrimes tão precária, voltamos ao projeto de lei 84/1999 que visava tornar crime doze tipos de ações praticadas na internet, passíveis de prisão e multa. Porém o projeto era considerado o verdadeiro AI-5 Digital, e mesmo anos depois, em 2008, seu texto não conseguia ser aprovado pela sua quantidade de brechas e pontos controversos. Assim, para que fosse aprovado em 2012 o texto acabou por ser vetado em diversos artigos importantes os quais tratavam sobre como punir quem invade computadores ou derruba sites e redes.

O questionamento é que dois anos depois da proposta do Projeto de Lei Azeredo é celebrada em Budapeste, na Hungria, a Convenção sobre Cibercrimes. Ela engloba países do mundo inteiro e tipifica os principais crimes cometidos na Internet e em outras redes informáticas, tratando de infrações de direitos autorais, fraudes informáticas, pornografia infantil e violações da segurança de rede, tudo em um só documento, porém, o Brasil ainda não participa da Convenção até os dias de hoje. A Convenção é composta por quatro capítulos e quarenta e oito artigos, ela é considerada de fácil compreensão por não trazer muitas questões técnicas.[78]

A Convenção tem como objetivo principal buscar maneiras rápidas e eficazes de acabar com as ameaças presentes no ciberespaço por meio da cooperação internacional penal. Em seu preâmbulo explicita que sua prioridade é de uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço. Uma norma que se mostra tão abrangente, buscando abarcar diversas legislações, com o interesse comum em encontrar um equilíbrio, uma regulamentação supranacional entre países para a resolução de cibercrimes, os quais ultrapassam

[78] **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em 03 mar. 2020.

fronteiras. Logo não há que se falar em cibercrimes sem que haja uma verdadeira cooperação entre nações.

Mas a Convenção, além de abordar direito processual, aborda principalmente matéria penal. No capítulo I define os cibercrimes, no capítulo II tipifica-os, como infrações contra sistemas e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com o conteúdo, pornografia infantil e as infrações relacionadas com a violação de direitos autorais.[79] Por mais que não seja o ideal e que a Convenção não vá suprir todas as lacunas legislativas, seria um norte importante na aplicação das leis, além, sobretudo, de ser um importante instrumento de cooperação internacional.

Na época, o Ministério das Relações Exteriores opôs-se expressamente à adesão do Brasil à Convenção. Alegava que não houve participação do Brasil na composição da redação do dispositivo, além de críticas feitas ao conteúdo da norma, alegando que nem todas as normas eram compatíveis com o ordenamento jurídico brasileiro vigente à época. [80]O Brasil possui uma tradição diplomática em não aderir acordos sobre os quais não foi convidado a discutir os termos.[81]Alegavam ainda que a adesão do Brasil à Convenção exigiria concessões importantes, como a possibilidade de interceptação de dados secretamente durante a comunicação de prestadores de serviços.[82]

Segundo o procurador Sérgio Suiama[83] a adesão traria vantagens como modelo legislativo homogêneo e a adoção de mecanismos de cooperação mais ágeis que a carta rogatória. Suiama lembra que foi por uma carta rogatória que demorou dois anos para que fosse possível conseguir um endereço de IP.

Para o Ministério Público Federal, a Convenção seria eficaz não só na resolução de casos de crimes cibernéticos, como, principalmente, na obtenção de provas digitais de forma ágil. Nos casos

---

[79] VOGT, Jackson. **Direito Cibernético: análise da legislação penal e a Convenção de Budapeste.** Disponível em: < https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/1531>. Acesso em: 07 jun. 2020.
[80] VOGT, Jackson. **Direito Cibernético: análise da legislação penal e a Convenção de Budapeste.** Disponível em: < https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/1531>. Acesso em: 07 jun. 2020.

[81] GROSSMANN, Luís. **Crimes Cibernéticos MPF pressiona por adesão à Convenção de Budapeste e a novo acordo com EUA.** Disponível em: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=48450&sid=4#:~:text=INTERNET-,Crimes%20Cibern%C3%A9ticos%3A%20MPF%20pressiona%20por%20ades%C3%A3o%20%C3%A0%20Conven%C3%A7%C3%A3o%20de%20Budapeste,a%20novo%20acordo%20com%20EUA&text=Vale%20lembrar%20que%20o%20Brasil,convidado%20a%20discutir%20os%20termos.>. Acesso em 25 jun. 2020.
[82] VOGT, Jackson. **Direito Cibernético: análise da legislação penal e a Convenção de Budapeste.** Disponível em: < https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/1531>. Acesso em: 07 jun. 2020.
[83] ERDELYI, Maria Fernanda. **Itamaraty ainda estua adesão à Convenção de Budapeste.** Disponível em: < https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em: 25 jun. 2020.

em que o crime praticado extrapola a jurisdição brasileira, a obtenção de informações se dá por meio de cooperação internacional, a qual deveria ser rápida e eficiente.[84] Mas não é o que acontece

Esse é um, dentre tantos outros motivos, que torna a adesão do Brasil à Convenção de Budapeste tão latente, pois, de acordo com o artigo 35 da Convenção os estados membros devem disponibilizar uma rede 24/7, ou seja, durante sete dias da semana, vinte e quatro horas por dia deve haver um ponto de contato para que todos os países membros possam prestar auxílio nas investigações e nos procedimentos relativos a infrações penais relacionadas aos crimes cibernéticos.

Uma das críticas feitas à época pela não adesão do Brasil à Convenção foi em relação ao prazo de armazenamento de informações por um provedor. Alegava-se que o prazo de noventa dias era inviável na lenta realidade judiciária brasileira.[85] Hoje em dia, esses prazos já foram exaustivamente debatidos para a elaboração do Marco Civil[86], que prevê a proibição da guarda de registros por parte dos provedores de conexão, como sites, blogs, fóruns e redes sociais e o prazo de seis meses nos casos de provedores de aplicação, com fins econômicos.

Quando se analisa a legislação brasileira à luz da Convenção de Budapeste podemos perceber que diversas condutas prescritas nesse documento já estão previstas no nosso ordenamento jurídico. O acesso e a interceptação ilegal são um exemplo, além da violação de direitos autorais e a falsificação de sistemas, todas já previstas e respaldadas em nossa legislação.[87]

O procurador Vladimir Aras chegou a afirmar em uma reunião para tratar sobre cooperação internacional do Brasil no combate aos crimes cibernéticos, ocorrida em 2018, que não há incompatibilidade entre o tratado e a legislação brasileira e que a interpretação de suas normas já está sendo construída por mais de 60 estados membros.[88]

---

[84] BRASIL. Ministério Público Federal. **MPF defende adesão do Brasil à convenão internacional para combate a crimes cibernéticos.** Disponível em: < https://mpf.jusbrasil.com.br/noticias/623847312/mpf-defende-adesao-do-brasil-a-convencao-internacional-para-combate-a-crimes-ciberneticos>. Acesso em: 26 jun. 2020.

[85] ERDELYI, Maria Fernanda. **Itamaraty ainda estua adesão à Convenção de Budapeste.** Disponível em: < https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em: 25 jun. 2020.

[86] BRASIL. **Lei 12.965, de 23 abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 26 jun. 2020.

[87] GOMES, Jefferson. **Sociedade da informação e a criminalidade informática as correlações entre a legislação brasileira e a Convenção de Budapeste sobre Cibercrimes.** Disponível em < http://repositorio.ufc.br/handle/riufc/26379>. Acesso em: 07 jun. 2020.

[88] BRASIL. Ministério Público Federal. **MPF defende adesão do Brasil à convenão internacional para combate a crimes cibernéticos.** Disponível em: < https://mpf.jusbrasil.com.br/noticias/623847312/mpf-defende-adesao-do-brasil-a-convencao-internacional-para-combate-a-crimes-ciberneticos>. Acesso em: 26 jun. 2020.

Além disso, na época, Azeredo dizia que o documento era controverso e que não existiam quaisquer indicativos de sucesso em relação a aplicação da norma. Hoje em dia, não é difícil perceber, que pela quantidade de países que aderiram a Convenção desde que ela foi celebrada no ano de 2001, a adesão não veio somente de países Europeus, mas de todo o globo.

Vale lembrar que a Convenção de Budapeste foi ratificada por diversos países, dentre eles países que abrigam grandes provedores e suporte de infra estrutura, como o Google, por exemplo. Os Estados Unidos ratificaram a convenção em 2008 com treze reservas à Convenção.[89]Conforme mencionado anteriormente, o Brasil ainda não faz parte da Convenção, mas em dezembro de 2019,[90] foi convidado pelo Comitê de Ministros do Conselho da Europa a aderir a Convenção sobre Crimes Cibernéticos, onde já pode participar como observador nas reuniões.

Compreende-se a importância de uma regulação do espaço sobre cibercrimes não só sob a ótica política da cooperação internacional, mas também sob o aspecto econômico, já que diversos países e empresas preocupam-se com a higidez e a segurança proporcionada pelo sistema jurídico brasileiro no combate ao cibercrimes para que mantenham relações com o Brasil.

Com isso, evidencia-se a necessidade de adesão do Brasil à Convenção de Budapeste em busca da necessária uniformização legislativa no combate aos crimes cibernéticos transnacionais, com um modelo homogêneo de aplicação para todos os países membros, possibilitando, assim, uma maior variedade de instrumentos aplicáveis sobre delitos informáticos, além de facilitar a cooperação internacional, por meio do sistema 24/7, tornando a obtenção e a cooperação de provas muito mais rápida, ágil e em tempo real. A norma só viria a somar ao ordenamento jurídico, juntamente com a Lei Carolina Dieckmann e principalmente ao Marco Civil da Internet.

CONSIDERAÇÕES FINAIS

O presente trabalho visou analisar a legislação brasileira no tocante ao ciberespaço, mas principalmente em relação aos cibercrimes, e a compatibilidade, mesmo que parcial, do ordenamento jurídico brasileiro com a Convenção de Budapeste. Para isso, foi imprescindível um estudo

[89] BRASIL. Ministério das Relações Exteriores. **PROCESSO de adesão à Convenção de Budapeste – Nota 309**. Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em: 04 maio 2020

[90] BRASIL. Ministério das Relações Exteriores. **PROCESSO de adesão à Convenção de Budapeste – Nota 309**. Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>. Acesso em: 04 maio 2020

aprofundado da Convenção sobre Cibercrimes, realizando uma análise desde a criação da Internet até a ratificação da Convenção, além de uma pesquisa histórica e normativa do arcabouço legal brasileiro.

Foi com o fim da Segunda Guerra Mundial que diversas tecnologias foram criadas, desenvolvidas e aprimoradas, com ela o surgimento da Internet, que na época era restrita ao uso militar. Com o passar dos anos a rede mundial de computadores se tornou um meio acessível, de um modo geral, a população, aproximando e encurtando distâncias.

Com a nova ferramenta disponível a uma grande parte de usuários, não demorou muito para que fosse necessário lidar com as benesses, mas também com as mazelas da rede. Foi nesse contexto que surgiu o termo cibercrime, seja ele impróprio ou próprio. Nesse novo ambiente, o virtual, foi facilitado o cometimento de crimes online, de forma rápida e instantânea, além do surgimento de novos delitos nunca antes regulamentados, e consequentemente sem punição, pois, não há crime sem lei anterior que o defina.

Com base nisso que se iniciou uma corrida penal punitiva, antes mesmo que se regulasse condutas civilmente. A preocupação do legislativo e do judiciário foi em criminalizar essas condutas praticadas no ciberespaço, porém, ainda não se tinha regulamentação alguma. E mesmo hoje em dia, após diversos esforços, e diversas leis criadas e alteradas, ainda restam lacunas legislativas. Paulo Rená[91] diz em sua dissertação de mestrado ser incoerente a proposta de uma norma penal antes mesmo da existência de uma legislação civil.

Foram exemplificados alguns marcos legislativos importantes para a consolidação de uma regulamentação do espaço cibernético e da cibercriminalidade. Inicialmente foi proposto o Projeto de Lei Azeredo, que por ser considerado o verdadeiro AI-5 Digital, não conseguia ser aprovado por sua rigidez. Anos mais tarde, por uma pressão social e política os temas ciberespaço, cibercriminalidade e cibersegurança voltam à tona e anseiam por regulamentação.

O projeto de lei 2.793/2011 consegue sua aprovação no ano de 2012 dando origem a Lei 12.737/2012, mais conhecida como Lei Carolina Dieckmann, juntamente com o antigo projeto de lei Azeredo, porém, só conseguiu sua aprovação após diversos pontos polêmicos serem retirados, dando origem a Lei 12.735. Alguns anos depois, em 2014, entrou em vigor o Marco Civil da Internet, Lei 12.965.

---

[91] SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>. Acesso em: 27 jun. 2020.

Mas, todos esses projetos de lei que buscavam de alguma forma regulamentar o ciberespaço ou a cibercriminalidade surgiram anos após a ratificação da Convenção sobre Cibercrimes. Ela foi celebrada no ano de 2001, em Budapeste, e já foi assinada por mais de sessenta países do globo, exatamente por seu teor ser do interesse de todos, prezando pelo equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais homem.

A Convenção de Budapeste buscou maneiras rápidas e eficazes para ameaças presentes no ciberespaço, utilizando-se da cooperação internacional, sendo o primeiro tratado internacional que buscou acordar a cibercriminalidade e harmonizar as legislações nacionais para que houvesse uma regulamentação única, supranacional e homogênea, pois não há como se falar em cibercrimes sem que haja uma cooperação internacional, uma verdadeira cooperação entre nações.

O Brasil não aderiu à Convenção sobre Cibercrimes na época por uma questão diplomática em não aderir acordos sobre os quais não foi convidado a discutir os termos. Além disso o Ministério das Relações Exteriores alegou que nem todas as normas eram compatíveis com o ordenamento jurídico brasileiro vigente à época, e que sua adesão exigiria concessões importantes.

Azeredo dizia que o a Convenção era controversa e que não existiam quaisquer indicativos de sucesso em relação a aplicação da norma. Tantos anos depois, e após o número de países-membros quase dobrar a Convenção é um sucesso, e demonstra atendar e todos, tanto aos países ocidentais, como os países orientais, todos em busca de um bem comum.

Porém, vimos que muitas dessas alegações já foram dirimidas em outras legislações criadas posteriormente, como o Marco Civil da Internet. E, após um comparativo foi possível perceber a compatibilidade do ordenamento jurídico brasileiro com a Convenção de Budapeste, que só viria a acrescentar a legislação brasileira, juntamente com outras leis, como a Lei Carolina Dieckmann, a Lei Azeredo, o Marco Civil, a E-Ciber, dentre outros.

REFERÊNCIAS

AGUIRRE, Lauriane. **Cibercrime como pauta da CPLP.** Disponível em: < https://ceiri.news/cibercrime-como-pauta-da-cplp/>.

ALMEIDA, Jéssica de Jesus. **Crimes cibernéticos**. Periódicos Grupo Tiradentes, v. 2, n.3. p. 215-236, 2015. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/viewFile/2013/1217>.

ALMEIDA, Sara. INFORPRESS. **Crimes cibernéticos têm aumentado exponencialmente a nível mundial e Cabo Verde não foge à regra – PCA da ARME.** Disponível em: https://expressodasilhas.cv/pais/2020/02/12/crimes-ciberneticos-tem-aumentado-exponencialmente-a-nivel-mundial-e-cabo-verde-nao-foge-a-regra-pca-da-arme/67934>.

BARRETO, Alessandro Gonçalves. **Análise da Lei Azeredo: necessidade de criação de delegacias e setores especializados na repreensão aos crimes informáticos.** Disponível em: < https://www.migalhas.com.br/depeso/278027/analise-da-lei-azeredo-necessidade-de-criacao-de-delegacias-e-setores-especializados-na-repreensao-aos-crimes-informaticos>.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012.** Revista Âmbito Jurídico. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>.

BRASIL. **Projeto de Lei 84, de 24 fev. 1999. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>.

BRASIL. **Projeto de Lei 2.793, de 29 nov. 2011. Dispõe sobre a tipificação criminal de** delitos informáticos e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>.

BRASIL. **Projeto de Lei 2.126, de 24 ago. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: < https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>.

BRASIL. **Lei 12.965, de 23 de abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. **Lei 12.737, de 30 nov. 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.

BRASIL. **Lei 12.735, de 30 nov. 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>.

BRASIL**. Lei no 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>.

BRASIL. **Lei 7.716, de 05 jan 1989. Define os crimes resultantes de preconceito de raça ou de cor.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l7716.htm >.

BRASIL. **Lei 11.829, de 25 nov 2008. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>.

BRASIL. **Decreto 10.222, de 05 fev 2020. Aprova a Estratégia Nacional de Segurança Cibernética.** Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>.

BRASIL. **Código Penal - Decreto-Lei 2.848, de 07 dez. 1940.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>.

BRASIL. Departamento de Segurança da Informação. **E-Ciber.** Disponível em: < http://dsic.planalto.gov.br/links-destaques/e-ciber>.

BRASIL. **Decreto 9.637, de 26 dez 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>.

BRASIL. **Decreto 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 24 jul. 2020.

[1] BRASIL. Decreto 8.135, de 04 de novembro de 2013. **Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em: 24 jul. 2020.

BRASIL. Ministério das Relações Exteriores. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública.** Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>.

BRASIL. Senado Notícias. **Brasil é o 2º no mundo em perdas por ataques cibernéticos, aponta audiência.** Disponível em: < https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>.

BRASIL. Ministério da Economia. **Organização para a Cooperação e Desenvolvimento Econômico – OCDE.** Disponível em: http://www.fazenda.gov.br/assuntos/atuacao-internacional/cooperacao-internacional/ocde>.

BRASIL. Senado Notícias. **Brasil é o 2º no mundo em perdas por ataques cibernéticos, aponta audiência.** Disponível em: < https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>.

BRASIL. Ministério Público Federal. **Fortalecer a cooperação internacional é essencial para enfrentar crimes cibernéticos, defende MPF.** Disponível em: < http://www.mpf.mp.br/pgr/noticias-pgr/fortalecer-a-cooperacao-internacional-e-essencial-para-enfrentar-crimes-ciberneticos-defende-mpf>.

BRASIL. Ministério Público Federal. **MPF defende adesão do Brasil à convenão internacional para combate a crimes cibernéticos.** Disponível em: < https://mpf.jusbrasil.com.br/noticias/623847312/mpf-defende-adesao-do-brasil-a-convencao-internacional-para-combate-a-crimes-ciberneticos>.

BRAGATTO, Rachel; SAMPAIO, Rafael; NICOLÁS, Maria. **A segunda fase da consulta do marco civil da internet: como foi construída, quem participou e quais os impactos?** In: Revista Eptic, vol. 17, nº 1, jan-abr 2015. Disponível em: < https://seer.ufs.br/index.php/eptic/article/view/3385>.

BEZERRA, Arthur; WALTZ, Igor. **Privacidade, Neutralidade e Inimputabilidade da Internet no Brasil: avanços e deficiências no projeto do Marco Civil.** In: Revista Eptic Online, vol. 16, n.2, p.161-175, mai-ago 2014. Disponível em: < https://ridi.ibict.br/bitstream/123456789/858/2/Arthur.pdf>.

CALIXTO, Larissa. **E-Ciber: governo determina uma série de padrões para segurança cibernética.** Disponível em < https://congressoemfoco.uol.com.br/governo/e-ciber-governo-determina-uma-serie-de-padroes-para-seguranca-cibernetica/?aff_source=56d95533a8284936a374e3a6da3d7996>.

CONGO, Mariana. **Lei Carolina Dieckmann e Lei Azeredo entram em vigor hoje; saiba onde denunciar.** Estadão, São Paulo, 2 de abr. 2013. Disponível em: <https://economia.estadao.com.br/blogs/radar-tecnologico/lei-carolina-dieckmann-e-lei-azeredo-entram-em-vigor-hoje-saiba-onde-denunciar/>.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime - ETS nº 185**. Disponível em < https://www.migliorisiabogados.com/que-paises-firmaron-y-ratificaron-la-convencion-mundial-contra-el-cibercrimen-budapest-2001/?lang=pt>.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime - ETS nº 189.** Disponível em <https://rm.coe.int/16802ed8cd>.

CONSELHO DA EUROPA. **Quadro de assinaturas e ratificações do Tratado - ETS nº 185 – Convenção sobre Cibercrimes.** Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>.

Convenção sobre o Cibercrime – Convenção de Budapeste. Budapeste, 23 nov. 2001. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>.

ERDELYI, Maria Fernanda. **Itamaraty ainda estua adesão à Convenção de Budapeste.** Disponível em: < https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>.

FABRO, Clara. **Golpe de roubo de dados bancários cresce e Brasil é um dos mais afetados.** Disponível em: < https://www.techtudo.com.br/noticias/2020/05/golpe-de-roubo-de-dados-bancarios-cresce-e-brasil-e-um-dos-mais-afetados.ghtml>.

GOMES, Jefferson. **Sociedade da informação e a criminalidade informática as correlações entre a legislação brasileira e a Convenção de Budapeste sobre Cibercrimes.** Disponível em < http://repositorio.ufc.br/handle/riufc/26379>.

GOMES, Rodrigo. **Interpol.** Disponível em <https://www.infoescola.com/geografia/interpol/>

GROSSMANN, Luís. **Crimes Cibernéticos MPF pressiona por adesão à Convenção de Budapeste e a novo acordo com EUA.** Disponível em: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=48450&sid=4#:~:text=INTERNET-,Crimes%20Cibern%C3%A9ticos%3A%20MPF%20pressiona%20por%20ades%C3%A3o%20%C3%A0%20Conven%C3%A7%C3%A3o%20de%20Budapeste,a%20novo%20acordo%20com%20EUA&text=Vale%20lembrar%20que%20o%20Brasil,convidado%20a%20discutir%20os%20termos.>.

.

HAJE, Lara. **Ministério Público pede rejeição de projeto que proíbe bloqueio do Whatsapp - Representantes do MP, de delegados e peritos defendem adesão do Brasil à Convenção de Budapeste sobre crimes cibernéticos.** Disponível em: <https://www.camara.leg.br/noticias/571408-ministerio-publico-pede-rejeicao-de-projeto-que-proibe-bloqueio-do-whatsapp/>.

KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet.** Conjur, 24 nov 2001. Disponível em: < https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes>.

LANDIM, Wikerson. **Conheça a Lei Azeredo, o SOPA brasileiro.** Disponível em: <https://www.tecmundo.com.br/ciencia/18357-conheca-a-lei-azeredo-o-sopa-brasileiro.htm>.

LÉVY, Pierre; **Cibercultura.** São Paulo: Ed. 34, 1999

LUCA, Cristina de. **Proposta de emenda constituinal diferencia segurança e defesa cibernética.** Disponível em: < https://porta23.blogosfera.uol.com.br/2020/02/16/proposta-de-emenda-constitucional-diferencia-seguranca-e-defesa-cibernetica/>.

MARTINS, AISLAN. **Crimes Virtuais.** Sabará 2017. Disponível em: <https://www.faculdadesabara.com.br/media/attachments/monografias/Monografia_Crimes-Virtuais_Aluno-Aislan.pdf>

NASCIMENTO, Samir de Paula. **Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais.** Disponível em: < https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>.

NETO, Arnaldo. **Cibercrime e Cooperação Penal Internacional: Um Enfoque à Luz da Convenção de Budapeste.** Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/arnaldo-sobrinho-cibercrime-e-cooperacao-penal-internacional.pdf >.

PINTO, Marcio. **O Direito da internet: o nascimento de um novo ramo jurídico**. Disponível em: <http://jus.com.br/revista/texto/2245>.

RICHTER, André. **Brasil inicia adesão a tratado contra crimes cibernéticos – Convenção de Budapeste permite acesso mais rápido a provas eletrônicas. Disponível em:** https://agenciabrasil.ebc.com.br/internacional/noticia/2019-12/brasil-inicia-adesao-tratado-contra-crimes-ciberneticos>.

SANTARÉM, Paulo Rená da Silva. **O Direito achado na rede – A emergência do acesso à Internet como direito fundamental no Brasil.** Disponível em: <https://hiperficie.files.wordpress.com/2011/04/dissertac3a7c3a3o-o-direito-achado-na-rede.pdf>.

SIMÕES, Lucas. **Ações sobre WhatsApp e Marco Civil da Internet estão em pauta no STF.** Disponível em < https://www.moneytimes.com.br/acoes-sobre-whatsapp-e-marco-civil-da-internet-estao-na-pauta-do-stf/>.

SOUZA, Ramon. **Hoje é o Dia Internacional da Proteção de Dados Pessoais**. Disponível em: <https://thehack.com.br/hoje-e-o-dia-internacional-da-protecao-de-dados-pessoais/>.

SCHJOLBERG, Stein. **The History of Global Harmonization on Cybercrime Legislation**

STF. **ADC 51 – Audiência Pública sobre controle de dados de usuários por provedores de internet no exterior.** Disponível em: < http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf.>

TATEOKI, Victor. **Classificação dos Crimes Digitais**. Disponível em: <https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais>.

TOKARNIA, Mariana. **Um em cada 4 brasileiros não tem acesso à internet.** Disponível em: < https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/um-em-cada-quatro-brasileiros-nao-tem-acesso-internet>.

VENTURA, Felipe. **Dieckmann x Azeredo: como se comparam os dois projetos de lei para crimes virtuais**. Disponível em: <https://gizmodo.uol.com.br/projeto-leis-dieckmann-azeredo/>.

VERONESE, Alexandre. **Cooperação jurídica e proteção de dados pessoais – A necessidade de inserção do Brasil nos tratados do Conselho da Europa.** Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunqas/judiciario-e-sociedade/cooperacao-juridica-e-protecao-de-dados-pessoais-12042019>.

VOGT, Jackson. **Direito Cibernético: análise da legislação penal e a Convenção de Budapeste.** Disponível em: < https://bibliodigital.unijui.edu.br:8443/xmlui/handle/123456789/1531>.