UNIVERSIDADE FEDERAL DO PARANÁ

BRUNO HENRIQUE ZANETTE MINSKI

CRIMES CIBERNÉTICOS E A RESPONSABILIDADE DOS PROVEDORES: Uma análise conceitual e legislativa sob a ótica da sociedade de informação e do risco

CURITIBA

2018

BRUNO HENRIQUE ZANETTE MINSKI

CRIMES CIBERNÉTICOS E A RESPONSABILIDADE DOS PROVEDORES: Uma análise conceitual e legislativa sob a ótica da sociedade de informação e do risco

Monografia apresentada ao curso de Graduação em Direito, Setor de Ciências Jurídicas, Universidade Federal do Paraná, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Paulo César Busato

CURITIBA

2018

À minha família, por todo o carinho e apoio prestados.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por todas as bênçãos concedidas ao longo dos anos, em especial pela possibilidade de ingresso na Universidade Federal do Paraná.

Agradeço também aos meus pais, Beti e Alaor, pelo imenso amor, paciência e cooperação entregues desde sempre, sem eles eu nada seria.

A meu irmão, Ricardo, por todo o carinho, além de ter aguentado minha ausência e cansaço por mais vezes do que eu gostaria de admitir.

Aos demais familiares, que sempre me deram todo o suporte necessário para meu desenvolvimento pessoal e profissional.

Agradeço à Luísa por toda compreensão, auxílio, carinho e paciência, pela parceria desenvolvida nos últimos anos, por ter tornado mais leves e agradáveis meus dias dentro e fora da Universidade.

Aos demais amigos que o Curso de Direito me apresentou, agradeço por terem me ajudado a evoluir como ser humano e como jurista.

Também, agradeço ao Prof. Dr. Paulo César Busato, por ter aceitado me orientar nessa jornada e por toda a atenção concedida durante a realização deste trabalho.

A todos, a minha mais profunda gratidão.

RESUMO

O presente trabalho toma por objeto de estudo os chamados “crimes cibernéticos”. A escolha do tema foi motivada pelo crescimento no número de delitos relacionados às novas tecnologias e pela falta de entendimento pacificado na doutrina a respeito deles. Assim, estabeleceu-se como objetivo a análise da especificidade desses crimes quando comparados aos delitos tradicionalmente tipificados, da necessidade de uma regulamentação jurídica própria ao tema, bem como da possibilidade de responsabilização dos provedores de Internet, no âmbito de sua colaboração com a Justiça. Nesse sentido, foi realizado, primeiramente, um exame do contexto no qual os cibercrimes estão inseridos, para, então, discorrer acerca a temática sob uma perspectiva conceitual e pautada em possíveis propostas de sistematização. Após, realizou-se um estudo sobre os pontos positivos e negativos do arcabouço legislativo pátrio concernente ao tema, mediante análise de diplomas tais como a Lei Carolina Dieckmann e o Marco Civil da Internet. Por fim, efetuou-se uma abordagem acerca da participação dos provedores na investigação desses delitos, bem como das possibilidades de responsabilização a que estão sujeitos tais agentes privados. Para tanto, empregou-se o método dedutivo de fonte indireta para a construção dos fundamentos textuais, baseado numa pesquisa doutrinária e legislativa a respeito do tema, com vistas a possibilitar uma análise crítica sobre as questões, reconhecendo os avanços, apontando os problemas subsistentes e ressaltando a importância do diálogo entre a teoria e a prática para o adequado tratamento da matéria.

Palavras-chave: Direito Penal. Crimes Cibernéticos. Lei n. 12.737/12. Lei n. 12.965/14. Provedores de Internet.

ABSTRACT

The present work takes as object of study the so-called "cybercrimes". The choice of theme was motivated by the increase in the number of crimes related to new technologies and by the lack of pacified understanding in the doctrine regarding them. Thus, the objective was to analyze the specificity of these crimes when compared to the crimes traditionally classified, the need for legal regulation specific to the subject, as well as the possibility of accountability of Internet providers, in the context of their collaboration with the Justice. In this sense, an examination was first made of the context in which cybercrimes are embedded, then to discuss the theme from a conceptual perspective and based on possible systematization proposals. Afterwards, a study was carried out on the positive and negative aspects of the legislative framework concerning the theme, through analysis of diplomas such as the Carolina Dieckmann Law and the Civil Internet Framework. Finally, an approach was taken on the participation of providers in the investigation of these crimes, as well as the possibilities of accountability to which such private agents are subject. For that, the indirect deductive method was used to construct the textual foundations, based on a doctrinal and legislative research on the subject, with a view to providing a critical analysis of the issues, recognizing the advances, pointing out the remaining problems and emphasizing the importance of the dialogue between theory and practice for the appropriate treatment of matter.

Keywords: Criminal Law. Cybercrimes. Law no. 12.737/12. Law no. 12.965/14. Internet Providers.

SUMÁRIO

INTRODUÇÃO

A proposta desta monografia é realizar uma análise a respeito dos chamados “crimes cibernéticos”. A escolha do tema foi motivada pelo crescimento no número de delitos relacionados às novas tecnologias e pela falta de entendimento pacificado na doutrina a respeito deles.

O presente estudo almeja realizar uma análise crítica do panorama atual, com base na verificação das particularidades dessa criminalidade e do modo como o ordenamento jurídico brasileiro tem regulado a matéria, com seus pontos positivos e negativos.

A pesquisa se revela pertinente devido à dificuldade em se encontrar obras, estudos e pesquisas sobre a temática. Verifica-se a necessidade de um aprofundamento no estudo dos crimes cibernéticos, não apenas com o intuito de aprimorar o entendimento jurídico teórico a respeito do fenômeno, mas também com vistas a auxiliar na efetiva investigação desses crimes, fundamentando a atuação das autoridades policiais.

Nesse sentido, busca-se tecer considerações a respeito da própria estrutura dos órgãos investigativos criminais, haja vista que grande parte dos Estados da Federação ainda não dispõe de uma estrutura especializada em tais delitos. Seja por falta de capacitação profissional, ou em razão da condição financeira material deficitária, constata-se que o enfrentamento prático dos cibercrimes está ainda muito aquém do que, em tese, deveria ser.

Com a definição e escolha do tópico de investigação foi necessário delimitar o problema. Esse estudo objetiva, em especial, a análise da especificidade desses crimes quando comparados aos delitos tradicionalmente tipificados, da necessidade de uma regulamentação jurídica própria ao tema e de sua configuração até o presente momento, bem como da possibilidade de responsabilização dos provedores de Internet, no âmbito de sua colaboração com a Justiça.

O método utilizado para a construção das principais ideias textuais foi o dedutivo de fonte indireta, pois o presente trabalho partiu de uma pesquisa geral acerca dos crimes cibernéticos, para então se atentar às legislações específicas, prosseguir na verificação das particularidades da investigação

desses delitos, culminando com o estudo das questões relativas aos provedores. Para tanto, partiu-se de uma pesquisa bibliográfica como fonte da construção de um marco teórico conceitual do estudo, além de legislações pertinentes à temática.

A estrutura da pesquisa se respalda, primeiramente, na análise contextual da criminalidade cibernética, marcada pelo advento da sociedade da informação e do risco, para então, realizar uma abordagem a respeito dos aspectos mais conceituais desses crimes e das propostas doutrinárias para sistematização do fenômeno.

O capítulo 2 possui como escopo essencial o exame da configuração contemporânea da legislação pátria em relação à temática em apreço, perpassando por diplomas como a Lei Azeredo, Lei Carolina Dieckmann, Marco Civil da Internet e, inclusive, a recente Lei 13.718/2018.

Por fim, no capítulo 3, aborda-se a questão da investigação desses delitos, na qual os provedores de Internet possuem um relevante papel. A partir disso, discute-se acerca das possibilidades de responsabilização desses agentes privados, verificando as atuais disposições brasileiras e complementando-as com considerações acerca do modelo adotado na Espanha.

1 CRIMES CIBERNÉTICOS: CONCEITOS E CATEGORIZAÇÕES

O advento de novas tecnologias proporcionou uma verdadeira metamorfose nas sociedades ao redor do globo, houve substanciais alterações na forma como a humanidade passou a se relacionar consigo mesma e com o ambiente à sua volta – desde as mais básicas interações interpessoais até complexos sistemas integrados de gestão do Estado. No entanto, com as novas tecnologias despontaram também novos riscos, muitos dos quais até então inimagináveis – dentre eles, os crimes cometidos no âmbito da informática.

Muitas são as polêmicas envolvendo tais delitos chamados de cibernéticos. A produção doutrinária acerca do tema é diversificada e, em grande medida, discrepante, subsistindo questionamentos quanto a natureza desses ilícitos, em relação à necessidade de uma regulamentação específica da matéria, acerca de quais seriam as melhores práticas persecutórias, dentre outros.

Seja como for, exige-se que a utilização do instrumental penal, no bojo de um Estado Democrático de Direito, seja feita de maneira cuidadosa, com respeito aos princípios que lhe sustentam, de modo a evitar, na maior medida do possível, a ocorrência de abusos e injustiças no enfrentamento a tais delitos.

Assim sendo, por mais que a criminalidade cibernética se revele uma ameaça crescente nas sociedades contemporâneas, seu estudo e regulamentação devem ser realizados de maneira ponderada, consciente, tomando sempre em conta as particularidades que circundam esses ilícitos.

Nesse sentido, o presente capítulo se propõe a analisar o fenômeno dos crimes cibernéticos, elencando as principais posições teóricas a respeito do tema – em especial quanto aos seus aspectos mais conceituais – evidentemente, sem desconsiderar o contexto social em que estão inseridos, de uma sociedade cada vez mais digital, em constante transformação.

1.1 SOCIEDADE DA INFORMAÇÃO E DO RISCO

É notório que a sociedade hodierna se caracteriza por uma progressiva integração com as novas tecnologias. A internet – anteriormente vinculada aos projetos de inteligência militar – passa a ser cada vez mais indispensável para a organização humana, do funcionamento do Estado ao contato interpessoal.

Nesse paradigma tecnológico e digital em que "[...] a informação flui a velocidades e quantidades há apenas poucos anos inimagináveis, assumindo valores sociais e econômicos fundamentais",[1] as inovações se disseminam pelas mais diversas áreas do conhecimento e se fazem presentes, indubitavelmente, na forma como agimos[2] e nos relacionamos.

A partir dessa complexa "sociedade da informação", segundo Castells, marcada pela lógica das redes, disseminação e convergência das mais distintas tecnologias,[3] múltiplas podem ser as considerações acerca das transformações pelas quais o mundo vem passando.

É possível destacar diversos pontos positivos derivados dessa revolução e evolução tecnológica. Atualmente, percebe-se que grande parte da população mundial se utiliza desse instrumental em seu cotidiano, seja para o lazer, para busca de conhecimento, ou até mesmo como meio de trabalho.

Permitiu-se a conservação, produção e propagação de conhecimentos das mais diversas áreas, possibilitando uma ampla troca de informações ao redor do globo. A internet, por exemplo, possibilitou o acesso facilitado a uma quantidade incomensurável de saberes, desde sites de idoneidade duvidosa até acervos acadêmicos das mais renomadas universidades.

---

[1] TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil**: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000, p. 03. Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/livroverde.pdf.

[2] Necessário destacar o início da chamada "Internet das Coisas", um novo paradigma tecnológico que, muito provavelmente, vai revolucionar o modo como interagimos com nossos bens. – LEMOS, André. **A Comunicação das Coisas. Internet das Coisas e a Teoria Ator-Rede**: Etiquetas de radiofrequência em uniformes escolares na Bahia. Apresentado no SimSocial, 2012. Salvador, Bahia, outubro, p. 26-27. Disponível em: http://roitier.pro.br/wp-content/uploads/2017/09/Andre_Lemos.pdf.

[3] CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. – Rio de Janeiro: Jorge Zahar Ed., 2003, p. 07-08.

Além disso, através dos avanços tecnológicos facilitou-se a comunicação direta entre indivíduos das mais distintas localidades,[4] criaram-se novas oportunidades de emprego e inovadoras possibilidades de negócios[5] - muitas delas até pouco tempo inimagináveis.

Também, propiciou-se um aprimoramento em áreas como a da saúde, na qual a tecnologia permitiu o desenvolvimento de procedimentos menos invasivos, diagnósticos mais precisos e tratamentos com maior grau de eficácia, ao menos para aqueles que conseguem ter acesso a tais recursos.[6]

Não obstante, é preciso reconhecer que tais inovações também acabaram por produzir efeitos adversos, todo um "elenco específico de ameaças ou perigos característicos da vida social moderna".[7]

Consoante entendimento proferido por Giddens, a despeito da tecnologia e da globalização gerarem significativos avanços no campo da segurança, constata-se, de mesmo modo, a proliferação de novos riscos em escala global.[8] Guerras com imenso poder destrutivo, tragédias ecológicas, crises econômicas e problemas de abastecimento são apenas alguns exemplos desse "novo perfil de risco" [9] citado pelo autor.

De modo semelhante, Beck considera que o atual nível de desenvolvimento produziu riscos sociais "numa medida até então desconhecida".[10] Segundo o autor, os riscos sempre existiram, em maior ou menor medida,[11] porém, modernamente seria possível observar um

---

[4] TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil**: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000, p. 06-14. Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/livroverde.pdf.

[5] CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede**: do conhecimento à ação política; Conferência. Belém (Por): Imprensa Nacional, 2005, p. 21-22. Disponível em: http://www.egov.ufsc.br/portal/conteudo/sociedade-em-rede-do-conhecimento-%C3%A0-ac%C3%A7%C3%A3o-pol%C3%ADtica.

[6] LORENZETTI, Jorge; TRINDADE, Letícia de Lima; PIRES, Denise Elvira de Pires; RAMOS, Flávia Regina Souza. Tecnologia, inovação tecnológica e saúde: uma reflexão necessária. Texto Contexto Enferm, Florianópolis, 2012 Abr-Jun; 21(2): 432-9, p. 436. Disponível em: http://www.scielo.br/pdf/tce/v21n2/a23v21n2.pdf.

[7] GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora UNESP, 1991, p. 99.

[8] Ibidem, p. 111-113.

[9] Ibidem, p. 99.

[10] BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Ed. 34, 2010, p. 23.

[11] Ibidem, p. 25.

universalismo das ameaças, com irradiação de seus efeitos para o planeta como um todo.[12]

A respeito dessa "sociedade de risco", Beck sintetiza:

> Os riscos e ameaças atuais diferenciam-se, portanto, de seus equivalentes medievais, com frequência semelhantes por fora, fundamentalmente por conta da *globalidade* de seu alcance (ser humano, fauna, flora) e de suas causas modernas. São riscos da modernização. São um *produto de série* do maquinário industrial do progresso, sendo *sistematicamente* agravados com seu desenvolvimento ulterior.[13]

Naturalmente, a dualidade entre a produção de efeitos positivos e negativos também alcançou o âmbito do Direito. Nas últimas décadas presenciamos em todo o globo, inclusive no Brasil, a estruturação de sistemas de tramitação eletrônica dos processos, o advento de novos tipos de negócios jurídicos,[14] mas, também, a ocorrência de um sem-número de delitos,[15] possibilitados pelas vias telemáticas.

Trata-se, portanto, de um panorama de "metamorfose do mundo", no qual o corpo social está sujeito a uma série de convulsões sociais, culturais e paradigmáticas, em que antigas certezas se esvaem em prol do surgimento de novos começos.[16] Conforme visto, o advento das novas tecnologias marcou profundamente o agir da sociedade contemporânea, seja proporcionando benefícios e facilidades cotidianas, ou então produzindo riscos em escala global.

Tais inovações acabaram por cosmopolitizar o mundo, suavizando as fronteiras formais e interligando, em grande medida, a ação humana – com

---

[12] BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Ed. 34, 2010, p. 43.
[13] Ibidem, p. 26.
[14] Talvez o exemplo mais marcante seja a organização do e-commerce, conforme destaca o magistrado Semy Glanz. – GLANZ, Semy. **Internet e Contrato Eletrônico**. Revista da EMERJ, v.1, n.3, 1998, p.94-95. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/revista03_94.pdf.
[15] O Brasil foi um dos países com maior número de ataques virtuais em 2017, conforme demonstra o estudo realizado pela empresa de segurança Symantec: Norton Cyber Security Insights Report Global Results. Disponível em: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.
[16] BECK, Ulrich. **A metamorfose do mundo**: como as alterações climáticas estão a transformar a sociedade. – Lisboa: Edições 70, 2016, pos. 92.

todos os benefícios e malefícios decorrentes dessa situação.[17] Esse contexto conflituoso – e eminentemente pessimista, haja vista os altos níveis de preocupação e desilusão frente aos problemas contemporâneos[18] – permite, porém, uma janela de reflexão, em que se questiona a ordem político-social posta e abre-se espaço para novas visões de mundo.[19]

De todo modo, cabe destacar que, de antemão, não seria possível caracterizar tais mudanças como positivas ou negativas. Segundo Beck, o caminho estaria em aberto, a depender das decisões e posições a serem adotadas, de um "risco mundial para a catástrofe" até um "catastrofismo emancipatório".[20]

Sendo assim, ressalta-se que a capacidade de prever as ameaças mais próximas gera uma oportunidade ímpar à sociedade atual, qual seja a de buscar soluções inovadoras, perspectivas diferenciadas, realmente alternativas ao senso comum.[21]

Nas palavras do autor:

> O risco global não é a catástrofe global. É a antecipação da catástrofe. Implica que está na hora de agir – de retirar as pessoas das suas rotinas e de libertar os políticos dos "condicionalismos" que alegadamente os cercam. O risco global é a sensação diária de insegurança que já não podemos aceitar. Abre-nos os olhos e dá-nos esperança. Este encorajamento é o seu paradoxo.[22]

Se a sociedade hodierna é caracterizada pela proliferação de perigos universalizantes - dentre os quais se insere a criminalidade cibernética e o risco da liberdade digital[23] - faz-se necessária a utilização desse instrumental tecnológico também em prol da busca de respostas inventivas, de modo a extrair "efeitos secundários positivos" mesmo de tais males.[24]

Nesse sentido, o presente trabalho se dedicará ao estudo dos denominados crimes cibernéticos, atentando-se, num primeiro momento, aos

---

[17] BECK, Ulrich. **A metamorfose do mundo**: como as alterações climáticas estão a transformar a sociedade. – Lisboa: Edições 70, 2016, Kindle Version, pos. 133-175.
[18] Ibidem, pos. 282-289.
[19] Ibidem, pos. 309-316.
[20] Ibidem, pos. 342-348.
[21] Ibidem, pos. 644.
[22] Ibidem, pos. 701.
[23] Ibidem, pos. 2235.
[24] Ibidem, pos. 92.

seus aspectos basilares e especificidades, para então dispor acerca da regulamentação legal da matéria e de outros temas lhe são conexos.

1.2 ABORDAGENS CONCEITUAIS DOS CRIMES CIBERNÉTICOS

A despeito do crescente número de ocorrências práticas, ainda não existe na doutrina ou jurisprudência uma formulação teórica pacífica acerca dos crimes cibernéticos. Diversas são as posições adotadas e os debates perpassam pela nomenclatura a ser utilizada, pelas peculiaridades de tais crimes frente aos demais, culminando na propositura de distintas propostas de classificação e sistematização dos referidos delitos.

Nesse sentido, propõe-se analisar algumas das principais formulações doutrinárias a respeito da matéria, atentando-se, sobretudo, acerca de seus aspectos basilares, com o intuito de averiguar se a criminalidade cibernética possui características singulares frente aos demais delitos, capazes de justificar uma regulamentação jurídica específica.

Conforme exposto, é possível destacar que não existe consenso nem quanto a nomenclatura despendida à temática. Crime digital,[25] informático,[26] cibernético,[27] são exemplos de termos comumente utilizados pela doutrina para designar tais condutas ilícitas.

Destaca-se que entre os autores brasileiros há uma prevalência da expressão “crimes informáticos”, sendo tal nomenclatura muitas vezes defendida com base em sua abrangência potencial. Sydow, por exemplo, entende informática como o saber relativo ao tratamento da informação mediante o emprego de computadores e outros dispositivos tecnológicos, razão pela qual compreende que a referida terminologia seria suficientemente ampla para abarcar não apenas os delitos atuais, mas igualmente os futuros,

---

[25] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo : Saraiva, 2011, p.49.

[26] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 20.

[27] ARAGÃO, David Farias de. **Crimes Cibernéticos na Pós-Modernidade**: direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil. 2015. Dissertação (Mestrado em Direito) – Pró-Reitoria de Pesquisa e Pós-Graduação, Universidade Federal do Maranhão, São Luís, p. 60. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/667.

derivados da utilização criminosa de tecnologias ainda incipientes ou não descobertas.[28]

De todo modo, não é possível ignorar a massiva utilização de outras expressões pela doutrina, como, por exemplo, a que classifica os crimes relacionados ao advento da Internet e de outras tecnologias da informação como sendo “cibernéticos”.

Tal vertente defende o emprego do referido termo, principalmente, em razão da ampla aceitação que este tem perante a comunidade global,[29] tanto na produção acadêmica,[30] quanto na Convenção de Budapeste – principal pacto multilateral acerca do tema.[31]

Em razão do exposto, entende-se que ambas as designações são válidas e assaz compreensíveis para identificar o fenômeno em questão. Todavia, com o intuito de padronizar o texto aos diplomas internacionais, o presente trabalho opta por se filiar aos argumentos da segunda vertente apresentada, denominando tais delitos como crimes cibernéticos ou cibercrimes.

A despeito das divergências nominais, verifica-se certa consonância entre os autores no sentido de considerar os cibercrimes como sendo delitos praticados contra as novas tecnologias da informação – tais como a Internet, dispositivos informáticos e bancos de dados – ou então perpetrados através de sua utilização.[32]

Em síntese, é possível compreendê-los como ilícitos intrinsecamente conexos ao advento da sociedade da informação contemporânea, haja vista

---

[28] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015, p. 56.

[29] WENDT, Emerson**. Inteligência cibernética**: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil, - São Paulo: Editora Delfos, 2011, p. 69.

[30] VERDELHO, Pedro. **The Effectiveness of International Co-operation against Cybercrime**: examples of good practice. Strasbourg,, 2008, p. 04 Disponível em: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF.

[31] HUNGRIA. **Convenção sobre o Cibercrime**. Aberta para assinatura em Budapeste, Hungria, em 22 de novembro de 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf.

[32] WANG, Qianyun. **A Comparative Study of Cybercrime in Criminal Law**: China, US, England, Singapore and the Council of Europe. Tese de doutorado. Erasmus University Rotterdam, Roterdã, 2016, p. 05. Disponível em: https://www.bibliotheek.nl/catalogus/titel.408161779.html/a-comparative-study-of-cybercrime-in-criminal-law--china--us--england/.

que incidem sobre suas ferramentas de processamento e transmissão de dados, compreendendo-as como meio de cometimento de delitos ou como o próprio alvo da conduta criminosa.[33]

Relacionam-se, portanto, com o chamado ciberespaço, um ambiente de convívio interpessoal único, marcado pela dinamicidade, descentralidade e constante mutabilidade,[34] quanto às informações a ele transmitidas, e também em relação às pessoas que nele interagem.

Nesse sentido, destaca-se que os crimes cibernéticos acabam por atentar, em maior ou menor medida, contra os valores basilares desse "ambiente informático",[35] quais sejam sua confidencialidade, integridade e disponibilidade.[36]

Em primeiro lugar, confidencialidade diz respeito ao sigilo das informações condicionadas nos aparatos informáticos, no sentido de não serem, a priori, públicas, de livre acesso a qualquer indivíduo. Trata-se de uma faceta particular, proprietária, em que o acesso restará condicionado a determinada forma de permissão ou legitimação.[37]

Integridade, por sua vez, relaciona-se à incolumidade[38] desses dados digitais, ao direito que seu proprietário tem de desfrutá-los sem qualquer modificação indesejada ou não autorizada por parte de terceiros. Desse modo, impõe-se que qualquer proposta de alteração de tais informações seja feita de maneira clara e transparente, de forma a permitir ao usuário ter plena ciência quanto aos efeitos que dela podem decorrer, possibilitando uma escolha consciente e devidamente autorizada.[39]

Por fim, disponibilidade visa garantir o amplo acesso do usuário aos dados que lhe pertencem ou lhe foram autorizados. Trata-se de um valor

---

[33] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015, p. 63.
[34] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo : Saraiva, 2011, p.45.
[35] SYDOW, op. cit., p. 70.
[36] Valores dispostos expressamente no preâmbulo da Convenção de Budapeste. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf
[37] SYDOW, op. cit., p. 71-72.
[38] Integridade que, de modo diverso ao que possa sugerir, não deve se aproximar da noção de materialidade física, tendo em conta que tais dados e sistemas não podem ser considerados como bens tangíveis, corpóreos, visto que necessitam de algum aparato tecnológico para reproduzi-los. Ibidem, p. 73.
[39] Ibidem, p. 74-75.

complementar aos anteriores, pautado na “segurança informática”, visto que de nada adianta o sigilo e a incolumidade de tais informações se o alcance delas restar impossibilitado em razão de embaraços e incômodos.[40]

Considerando a relevância ímpar que as novas tecnologias detêm na sociedade atual, tem-se defendido que a proteção dos sistemas e dados informáticos teria alcançado um grau superior de importância,[41] equivalendo-se a outros bens e valores tradicionalmente caros ao corpo social, tal como o meio ambiente.[42]

Nesse sentido, a doutrina tem se manifestado no sentido de reconhecer que, dessa complexa relação entre humanidade e tecnologia, teriam surgido novos bens jurídicos, notáveis o bastante para receber a salvaguarda por parte do Estado, inclusive através da utilização do instrumental penal.[43]

Sendo assim, é possível verificar que os crimes cibernéticos distinguem-se de outros delitos não apenas pela utilização de ferramentas tecnológicas, mas, principalmente, em razão de se relacionarem a novos bens jurídicos, derivados da revolução informática.[44]

Ainda que não exista um rol taxativo de quais seriam os bens jurídicos informáticos, os autores convergem suas teses nas noções de inviolabilidade,[45] integridade[46] e segurança[47] desses dados ou sistemas.

Vianna e Machado, por exemplo, conferem maior destaque à inviolabilidade das informações digitais propriamente ditas, haja vista que, segundo eles, esta seria uma decorrência dos direitos à intimidade e privacidade, previstos expressamente no artigo 5º[48] da Constituição Federal.[49]

---

[40] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015, p. 76.

[41] Jesus e Milagre consideram que os dados informáticos foram elevados a um status de “valor jurídico fundamental” na sociedade atual, haja vista a crescente dependência dos indivíduos e instituições a tais informações. JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 35.

[42] SYDOW, op. cit., p. 79.

[43] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo : Saraiva, 2011, p.56.

[44] Ibidem, p. 57.

[45] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 20.

[46] CRESPO, op. cit., p. 57.

[47] SYDOW, op. cit., p. 84.

[48] Conforme dispõe o art. 5º, X, CF88: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de

Crespo, de outro modo, entende que a tutela jurisdicional também deveria ser estendida à segurança dos sistemas e redes informáticas, tendo em vista o caráter essencial que estes possuem nos dias de hoje.[50]

De todo modo, verifica-se uma tendência da doutrina em se filiar a um entendimento mais amplo, abarcando não somente os dados, mas também seu "receptáculo" - os computadores, sistemas em rede e demais dispositivos informáticos. Tal posição se fundamenta na inexistência de uma correlação estrita entre os componentes digitais e materiais, visto que a afronta às informações digitais não necessariamente resultaria em danos ao aparelho que as armazena (e vice-versa).[51]

Portanto, mesmo com eventuais divergências teóricas, evidencia-se que os crimes cibernéticos apresentam particularidades e singularidades frente a outros tipos penais tradicionalmente previstos no sistema penal, razão pela qual exigem um tratamento jurídico cuidadoso e específico.

Pelos motivos expostos, compreende-se como essencial o aprofundamento no estudo da matéria. Sendo assim, o presente trabalho passará a tratar sobre as possibilidades de classificação e sistematização dos cibercrimes propostas pela doutrina, as quais serão de grande valia para a posterior análise da legislação brasileira atinente à temática.

1.3 PROPOSTAS DE SISTEMATIZAÇÃO

Superadas as considerações iniciais acerca dos fundamentos e particularidades que caracterizam os crimes cibernéticos, prossegue-se ao estudo das propostas de sistematização da matéria. Porém, de mesmo modo, inexistente na doutrina qualquer consenso acerca de qual seria o modelo mais

---

outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm

[49] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 13.

[50] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo: Saraiva, 2011,p. 56.

[51] WANG, Qianyun. **A Comparative Study of Cybercrime in Criminal Law**: China, US, England, Singapore and the Council of Europe. Tese de doutorado. Erasmus University Rotterdam, Roterdã, 2016, p. 251. Disponível em: https://www.bibliotheek.nl/catalogus/titel.408161779.html/a-comparative-study-of-cybercrime-in-criminal-law--china--us--england/.

adequado para a classificação e o consequente enfrentamento dessa criminalidade cibernética.

Dessa forma, de modo a melhor esmiuçar as particularidades que a temática apresenta, o presente trabalho se atentará às três propostas de categorização mais difundidas, que contam com maior aceitação entre os autores brasileiros.

Partindo de uma estrutura bipartida, parte considerável da doutrina subdivide os delitos cibernéticos em dois grandes grupos: crimes próprios e impróprios, sendo estes relacionados a bens jurídicos tidos como tradicionais e aqueles ligados a bens jurídicos puramente informáticos.[52]

Nesse sentido, os crimes cibernéticos próprios seriam aqueles diretamente vinculados ao advento das novas tecnologias, inovadores no sentido de afrontarem bens jurídicos inerentes à sociedade do risco e da informação, tais como a inviolabilidade de sistemas informáticos e a integridade de suas informações.[53]

Nos crimes impróprios, por sua vez, as inovações tecnológicas seriam utilizadas meramente como meio ou instrumento para a realização de delitos "convencionais", haveria apenas uma inovação no *modus operandi* de cometimento de crimes devidamente tutelados pelo sistema penal. A título de exemplo, citam-se os crimes contra a honra, ameaça, falsidade ideológica, estelionato e tantos outros cometidos através da internet.[54]

Como dito, não há consenso quanto às propostas de categorização dos crimes cibernéticos. Assim, outra parcela da doutrina considera mais adequada uma classificação tripartida para tratar desses delitos.

Assim, por exemplo, seria possível subdividi-los em crimes de violação do meio informático através de ferramentas comuns; de violação do meio informático por meio de ferramentas exclusivamente informáticas; e de utilização dos meios informáticos para o ataque a bem jurídico de natureza diversa.[55]

---

[52] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo: Saraiva, 2011, p. 62.
[53] Ibidem, p. 57
[54] Ibidem, p. 91
[55] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015, p. 65.

Percebe-se que tal proposta realiza uma análise mais minuciosa acerca dos crimes cometidos contra os bens informáticos - seus sistemas e informações - visto que reconhece expressamente a possibilidade de a ofensa se valer tanto de meios físicos, corpóreos, quanto de ferramentas digitais.

Assim, na primeira categoria seriam inseridas as condutas de ataque aos sistemas informáticos por vias comuns, "analógicas", abarcadas por tipos penais já existentes. Nesse sentido, a destruição física de máquinas e servidores, por exemplo, afrontaria também a integridade desses dados, porém, através de um crime dano, possibilitando a aplicação imediata do Código Penal.[56]

No segundo conjunto, estariam previstos casos de hacking de dispositivos tecnológicos, inserção de códigos maliciosos, instalação de backdoors, derrubada de servidores via DoS etc., em que a afronta a tais bens jurídicos ocorreria por meio das próprias inovações informáticas[57] - contra as quais, muitas vezes, não há qualquer previsão legal.

Por fim, a última categoria diria respeito à utilização do instrumental tecnológico para a prática de crimes diversos, cujos bens jurídicos afligidos não seriam os informáticos. Portanto, trata-se de uma definição similar àquela dos crimes impróprios, nas quais a informática se apresenta tão somente como uma forma inovadora para a prática de delitos tradicionais ao sistema penal.[58]

A despeito das formulações sistêmicas previamente expostas, é possível também destacar uma terceira posição doutrinária, mais extensiva, a qual propõe quatro classes de crimes cibernéticos, quais sejam: próprios, mistos, mediatos e impróprios.[59]

De modo semelhante ao previamente exposto, os crimes próprios objetivariam a violação aos sistemas e suas informações digitais mediante o emprego de instrumentos tecnológicos, ou seja, tratar-se-iam de delitos

---

[56] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015, p. 65.
[57] Idem.
[58] Idem
[59] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 31-32.

distintos aos tradicionalmente previstos no Código Penal, com afronta a bens jurídicos singulares, derivados do advento da expansão informática.[60]

Os crimes mistos, por sua vez, seriam crimes em sua essência complexos, haja vista que afligiriam não apenas bens jurídicos informáticos - tais como a inviolabilidade das informações[61] - mas, igualmente, produziriam efeitos negativos a algum bem jurídico de natureza diversa.[62]

Em relação aos cibercrimes mediatos (ou indiretos), seria possível caracteriza-los como crimes-fim não cibernéticos, cujas realizações dependeriam de um anterior crime-meio de natureza cibernética.[63]

De outro modo, seriam delitos "clássicos", visando a afronta a bens jurídicos tradicionais, mas cuja forma de realização dependeria, necessariamente,[64] de um prévio ilícito cibernético – como exemplo, seria possível citar o caso de invasão de dispositivo eletrônico, com captura de dados bancários alheios, com vistas a furtar os proveitos da vítima.[65]

Finalmente, tal vertente também se vale da noção de crimes cibernéticos impróprios, nos quais os aparatos tecnológicos se apresentariam como meio alternativo, dentre os vários possíveis, para a realização de delitos já tipificados no ordenamento jurídico pátrio.[66]

Por mais variadas que sejam as propostas de categorização dos crimes cibernéticos elencadas pela doutrina, verifica-se uma constância de duas grandes classes de delitos: aqueles em que se atenta contra bens jurídicos tidos como inerentes à tecnologia da informação e, de outro modo, aqueles nos quais o aparato informático é utilizado apenas como ferramenta para a prática de infrações clássicas, violando bens jurídicos das mais diversas naturezas.

---

[60] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 35.

[61] Apenas a título de exemplificação, seria possível citar o artigo 67, VII da Lei nº 9.100/95, na qual a invasão de dispositivo vinculado ao sistema eleitoral tem por objetivo alterar a apuração ou contagem de votos. BRASIL. **Lei nº 9.100**, de 29 de setembro de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9100.htm.

[62] VIANNA; MACHADO, op. cit., p. 32.

[63] Nas palavras de Vianna e Machado, "Crime informático mediato ou indireto é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação". Ibidem, p. 39.

[64] Por tal motivo, defende-se que a consumação de tal crime-fim deveria, consequentemente, absorver a prática do anterior crime-meio cibernético, haja vista a aplicação do princípio da consunção. Ibidem, p. 39.

[65] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 122.

[66] VIANNA; MACHADO, op. cit., p. 32.

A partir do exposto, por mais que a vertente bipartida tenda a uma simplificação demasiada do tema, sua precisão na identificação dos principais ilícitos praticados no âmbito digital, aliado à grande popularidade que possui entre os autores, faz dela a posição teórica adotada no presente trabalho.

Conforme destacado anteriormente, entende-se que nos crimes cibernéticos impróprios haveria apenas uma inovação no modo de realização de delitos já tipificados pelo sistema penal, tratar-se-iam de "velhos crimes com nova roupagem".[67] Assim, compreende-se que no trato a tais ilícitos seria suficiente a aplicação do arcabouço penal existente, com plena incidência das regras já positivadas no ordenamento jurídico brasileiro.

Acerca desse ponto, Aragão destaca:

> É importante ressaltar que para os crimes cibernéticos impróprios é possível a aplicação da legislação penal vigente, pois, como já se disse, trata-se simplesmente de técnica nova para cometimento de delitos que já existem, não havendo que se falar em violação ao princípio da analogia em malam partem. O Supremo Tribunal Federal, ao julgar os primeiros casos de crimes cibernéticos impróprios no HC nº 76689[68], entendeu que o meio técnico pode ser posterior à edição da lei, comparando o caso ao crime de homicídio, pois não foi necessária sua redefinição após a invenção da pólvora, tratando-se meramente de nova técnica [...].[69]

Conquanto, diverso é o panorama em relação aos crimes cibernéticos próprios. Em razão de se relacionarem a toda uma nova sorte de bens jurídicos - conectados intrinsecamente ao desenvolvimento tecnológico e à sua profunda assimilação pelo corpo social – tais ilícitos não podem ser conformados aos tipos penais classicamente previstos, sob pena de violação ao princípio basilar da estrita legalidade no Direito Penal.

---

[67] TRUZZI, Gisele; DAOUN, Alexandre. **Crimes informáticos**: o direito penal na era da informação. In: Proceedings of the Second Internacional Conference of Forensic Computer Science, Guarujá (SP), ABEAT, 2007, p. 118. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf.

[68] BRASIL. Supremo Tribunal Federal. **Habeas Corpus nº 76.689 - PB** – 1ª Turma. Distrito Federal. Relator: Min. Sepúlveda Pertence. Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo130.htm.

[69] ARAGÃO, David Farias de. **Crimes Cibernéticos na Pós-Modernidade**: direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil. 2015. Dissertação (Mestrado em Direito) – Pró-Reitoria de Pesquisa e Pós-Graduação, Universidade Federal do Maranhão, São Luís, p. 62. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/667.

Desse modo, constata-se a existência de uma verdadeira lacuna de punibilidade, visto que diversas condutas – muitas delas altamente danosas – ainda seguem tidas como atípicas no Direito brasileiro, em razão da inexistência de um instrumental específico e robusto acerca do tema.[70]

A sugestão do desenvolvimento de leis específicas para a regulamentação da matéria conduz, necessariamente, à relevante discussão acerca do "inchaço" do Direito Penal. Nos últimos anos, verificou-se uma intensa produção legislativa - inclusive no âmbito criminal - resultando na tipificação de toda uma sorte de condutas,[71] muitas das quais poderiam ser satisfatoriamente reguladas por meio de outros ramos do Direito, com mecanismos menos agressivos frente aqueles que o instrumental penal dispõe.[72]

Nesse sentido, parcela dos autores[73] defende que não haveria a necessidade do desenvolvimento de novas leis específicas a respeito dos crimes cibernéticos, sob o argumento de que o arcabouço legislativo não precisaria ser elastecido, mas apenas levemente ajustado, de modo a se modernizar e possibilitar um adequado tratamento da matéria.

Evidente que o Direito Penal não pode ser empregado – e especialmente, ampliado - de maneira desatenciosa. Ao contrário, o manejo de tal instrumental deve ser criterioso, recaindo tão somente às condutas tidas como mais intoleráveis no seio de determinada sociedade,[74] de modo a cumprir verdadeiramente com seu papel de *ultima ratio* do sistema jurídico nacional.[75]

Por mais que os crimes cibernéticos impróprios possam ser adequadamente enfrentados através das disposições já existentes no sistema penal, resta evidente, com base no exposto no presente capítulo, que os cibercrimes próprios possuem uma série de particularidades e originalidades

---

[70] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo: Saraiva, p. 45.
[71] TRUZZI, Gisele; DAOUN, Alexandre. **Crimes informáticos**: o direito penal na era da informação. In: Proceedings of the Second Internacional Conference of Forensic Computer Science, Guarujá (SP), ABEAT, 2007, p. 119. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf.
[72] MUÑOZ CONDE, Francisco; GARCÍA ARÁN, Mercedes. **Derecho Penal**: parte general – 8. ed. – Valência: Tirant Lo Blanch, 2010, p. 79.
[73] TRUZZI; DAOUN, op. cit., p. 119-120.
[74] MUÑOZ CONDE; GARCÍA ARÁN, op. cit., p. 72.
[75] BUSATO, Paulo César. **Direito penal**: parte geral. – 2. ed – São Paulo: Atlas, 2015, p. 55-56.

frente aos delitos comumente tipificados, razão pela exigem uma regulamentação específica.[76]

Nesse sentido, não se defende uma produção legiferante extensa e exaustiva acerca do tema. Em realidade, almeja-se que, mediante uma atenta análise do fenômeno, as eventuais inovações legislativas futuras possam regulamentar a matéria de forma eficiente, oferecendo soluções concretas e capazes de minimamente subsistir ao advento de novas tecnologias. Obviamente, que em conformidade com os princípios e garantias basilares ao sistema penal.[77]

Desse modo, ainda que ordenamento jurídico brasileiro já possua algumas leis que versam sobre a temática da criminalidade cibernética, é preciso destacar a incipiência de tal produção legal, haja vista que, além de diminuta, apresenta-se repleta de lacunas e ambiguidades, dificultando o enfrentamento prático desses delitos, conforme se passará a expor.

[76] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 50.
[77] BORTOT, Jessica Fagundes. **Crimes Cibernéticos**: aspectos legislativos na persecução penal com base nas legislações brasileira e internacional. Virtuajus (PUCMG), v. 13, 2017, p. 359. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745.

2 CONFIGURAÇÃO CONTEMPORÂNEA DA LEGISLAÇÃO PÁTRIA

Conforme exposto, os cibercrimes possuem uma série de particularidades e originalidades frente aos delitos comumente tipificados no ordenamento jurídico, por tal razão, preconiza-se uma regulamentação mais específica da matéria. No entanto, a produção legislativa acerca dos crimes cibernéticos no Brasil é bastante recente, sendo que apenas nos últimos anos foram promulgadas leis diretamente relacionadas com a temática.

De todo modo, antes de adentrar especificamente nas legislações mais recentes, é importante perpassar, ainda que brevemente, por diplomas precedentes que, embora não tenham tratado especificamente dos cibercrimes, trouxeram contribuições no campo da Internet e das novas tecnologias.

Assim, em 1998, promulgou-se a Lei n. 9.609, tendo como principal objetivo a proteção da propriedade intelectual dos softwares. Tal legislação, em consonância com disposições internacionais, estabeleceu definições técnico-jurídicas para tais programas informáticos, determinou direitos aos desenvolvedores, garantias aos usuários, além das respectivas infrações contra eventuais abusos.[78]

Destaca-se, porém, que o referido diploma se estruturou, eminentemente, sob a ótica do direito autoral, centralizando suas disposições em aspectos formalistas e mercantis, tais como extensão da tutela de autoria, registro em entidades governamentais, contratos de licença de uso e comercialização, dentre outros. Tal opção ficou também evidente no ponto relativo às infrações e penalidades, visto que a lei pouco dispôs acerca de violações diretas a esses softwares, tendo optado pelo enfoque na proteção dos direitos do autor.[79]

Dois anos após, a Lei n. 9.983/00 promoveu uma série de alterações ao Código Penal, dentre as quais a elaboração dos artigos 313-A e 313-B, os

---

[78] BRASIL. **Lei nº 9.609**, de 19 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm.

[79] A título de exemplo, cita-se o caput do artigo 12 da referida lei: Violar direitos de autor de programa de computador: Pena - Detenção de seis meses a dois anos ou multa. Idem.

quais visam resguardar os dados e os sistemas informáticos da Administração Pública, respectivamente.[80]

Em primeiro lugar, previu-se a responsabilização criminal do funcionário público autorizado que inserir ou facilitar a inserção de dados falsos, ou então que alterar ou excluir indevidamente dados corretos contidos nesses sistemas, com o fim de angariar vantagem ou causar dano.[81]

Por mais que se possa questionar a opção por um crime de perigo abstrato,[82] é preciso realçar a postura arrojada do legislador, no sentido de buscar a proteção da integridade desses dados informáticos, reconhecendo a importância deles para a adequada prestação da atividade administrativa.

De modo complementar, o artigo 313-B tipificou a modificação ou alteração não autorizada realizada por agentes públicos dos sistemas e programas informáticos utilizados pela Administração.[83] Ainda que a redação do dispositivo apresente diversas falhas,[84] novamente trata-se de uma interessante inovação legislativa.

No ano de 2008, sobreveio a Lei n. 11.829, cuja promulgação teve o intuito de aprimorar o combate à produção, venda e distribuição de material pornográfico infantil.[85] Para tanto, atualizou o Estatuto da Criança e do Adolescente, prevendo expressa responsabilização para as condutas praticadas através das tecnologias informáticas.[86]

---

[80] BRASIL. **Lei nº 9.983**, de 14 de julho de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9983.htm.

[81] Artigo 313-A, CP: "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

[82] BUSATO, Paulo César. **Direito penal**: parte geral. – 2. ed – São Paulo: Atlas, 2015, p. 466.

[83] Artigo 313-B (caput), CP: Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

[84] BUSATO, op. cit., p. 472-473.

[85] BRASIL. **Lei nº 11.829**, de 25 de novembro de 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm.

[86] Dentre as inovações, a referida lei introduziu o artigo 241-A no ECA, o qual dispõe em seu caput: "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". BRASIL. **Lei nº 11.829**, de

Inclusive, cabe destacar que o referido diploma prevê possibilidade de penalização do responsável legal pela prestação do serviço, caso este, ainda que oficialmente notificado, opte por não desabilitar o acesso ao conteúdo de pornografia infantil.[87]

Conforme exposto, apesar de o sistema penal apresentar algumas regulamentações, em maior ou menor medida, relativas à temática dos crimes cibernéticos, verifica-se que tal conjunto de leis ainda padecia de maior amplitude, tendo sua aplicação particularizada a tipos penais específicos ou agentes determinados.

Nesse sentido, observa-se uma alteração operacional a partir do ano de 2012, no qual foram introduzidas no ordenamento jurídico brasileiro leis diretamente relacionadas à criminalidade cibernética – com especial enfoque nos cibercrimes próprios. Por tal motivo, passa-se a uma análise mais detalhada de tais recentes diplomas, quais sejam as leis n. 12.735/12, 12.737/12, 12.965/14 e 13.718/18.

2.1 “LEI AZEREDO” (Lei n. 12.735/12)

A Lei n. 12.735/12, popularmente conhecida como “Lei Azeredo”, teve sua criação derivada do Projeto de Lei n. 84/99,[88] o qual gerou polêmicas quanto ao tom de suas propostas a respeito dos crimes, penas e procedimentos investigativos relacionados ao âmbito digital.

Inicialmente elaborado pelo ex-deputado federal Luiz Piauhylino e alterado posteriormente por Eduardo Azeredo, o referido PL sofreu diversas alterações durante seus mais de 13 anos de tramitação no Congresso Nacional. Chegou inclusive a ser apelidado de “AI-5 Digital” por parcela de

---

25 de novembro de 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm.

[87] Assim passou a dispor o parágrafo 2º do artigo 241-A, ECA: “As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo”. Idem.

[88] BRASIL. **Projeto de Lei nº 84, de 1999**. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=23342A6D4FB1ED35373900C1A5590713.node2?codteor=1034065&filename=Avulso+-PL+84/1999.

seus críticos,[89] sob o argumento de que seu texto se valia de uma linguagem demasiadamente imprecisa, possibilitando afrontas à liberdade e privacidade dos usuários da Internet.[90]

De sua redação original, que contava com dezoito artigos, sobreveio uma legislação enxuta - a Lei n. 12.735/12 – que acabou por abandonar muitas das disposições inicialmente previstas.

Seu texto definitivo promoveu breves alterações no Código Penal, no Código Penal Militar e na Lei n. 7.716/89, relativa aos crimes resultantes de preconceito. De todo modo, destaca-se que não houve o acréscimo de qualquer tipo penal no ordenamento jurídico pátrio.[91]

Dentre as principais inovações, o artigo 4º previu a criação de setores especializados, na estrutura das polícias judiciárias, aptos a atuar contra a "ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado".[92]

Essa disposição foi de extrema importância no aprofundamento dos estudos acerca do tema. A exigência da particularização estimulou a proliferação de centros policiais, ao longo de todo o país, voltados à investigação específica dos crimes cibernéticos, desenvolvendo novas estratégias e tecnologias no trato a esses delitos.[93]

A título de exemplificação, instituiu-se, no âmbito do Paraná, o Núcleo de Combate aos Cibercrimes (NUCIBER), o qual é responsável pela centralização das investigações, em todo o Estado, a respeito de tais delitos.

---

[89] Tal como demonstra a reportagem "**AI-5 digital ou PL Azeredo** – vigilantismo e violação de direitos", publicada no site nossoquintal.org. Disponível em: https://nossoquintal.org/2009/05/13/ai-5-digital-ou-pl-azeredo-%E2%80%93-vigilantismo-e-violacao-de-direitos/.

[90] BORTOT, Jessica Fagundes. **Crimes cibernéticos**: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. VirtuaJus, Belo Horizonte, v. 2, n. 2, p. 338-362, 2017, p. 350. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/download/15745/15745-56007-1.

[91] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 64.

[92] BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.

[93] WENDT, Emerson. **Inteligência cibernética**: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil, - São Paulo: Editora Delfos, 2011, p. 73.

Mesmo contando com uma equipe diminuta,[94] o NUCIBER se destaca como uma referência entre esses órgãos especializados. Sua posição centralizada permite uma análise macro dos problemas, bem como estimula a adoção de estratégias padronizadas a serem seguidas em todo o território paranaense.[95]

Todavia, insta ressaltar que a maioria dos Estados da Federação não dispõe de estruturas de semelhante porte, seja por falta de capacitação profissional, ou em razão da condição financeira material deficitária, fato é que o enfrentamento prático aos crimes cibernéticos está ainda muito aquém do que, em tese, deveria ser.[96]

Nesse sentido, Wendt e Jorge destacam o problema crucial da falta de integração entre os órgãos investigativos criminais. Segundo os autores, a falta de uma cultura de compartilhamento atrelada à evidente precariedade estrutural prejudica a troca de informações entre municípios e entre Estados, impossibilitando a construção de uma rede nacional frente à criminalidade cibernética.

Como mencionado, a "Lei Azeredo" também acabou por modificar a Lei n. 7.716/89, mormente em seu o artigo 20, §3º, II, no sentido de prever a possiblidade de "cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio", cujas manifestações possuam teor discriminatório ou preconceituoso.[97]

Ou seja, apesar de sucinta, tal disposição possibilitou a ampliação do âmbito de atuação contra essas manifestações discriminatórias, enquadrando as novas tecnologias em um rol até então composto apenas pelos veículos midiáticos tradicionais.

Como visto, apesar de ter produzido benefícios na tratativa da criminalidade cibernética – com destaque para a exigência da instituição de centros especializados, para investigação e estudo desses delitos - verifica-se

---

[94] Contingente que necessitaria ser reforçado para melhor atender ao volume de demandas, conforme se verifica no Ofício 790/16 – NUCIBER/DIC/DPC, 2016, p. 03-04. Disponível em: http://www.camara.gov.br/sileg/integras/1452406.pdf.

[95] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013, p. 252-253.

[96] Ibidem, p. 253.

[97] BRASIL. **Lei nº 7.716**, de 5 de janeiro de 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716.htm.

que a Lei n. 12.735/12 foi bastante discreta na abordagem da temática, sobretudo quando comparada às outras legislações que a sucederam, como por exemplo, a Lei n. 12.737/12.

2.2 “LEI CAROLINA DIECKMANN” (Lei n. 12.737/12).

A Lei n. 12.737/12 derivou de um Projeto de lei mais recente – de número 2.793/11 - apresentado no Congresso como proposta alternativa ao até então polêmico PL n. 84/99, sob a justificativa de que este traria “propostas de criminalização demasiadamente abertas e desproporcionais”, capazes de alcançar condutas legítimas e corriqueiras praticadas na Internet, trazendo riscos aos direitos dos usuários da rede.[98]

Não obstante a relevância de suas disposições, o PL n. 2.793/11 teve uma tramitação rápida dentro das Casas legislativas, principalmente quando comparado a outros projetos similares. O vazamento das fotos íntimas da atriz Carolina Dieckmann, em maio de 2012, teve o condão de agilizar as negociações e tratativas acerca da matéria, promovendo a “toque de caixa” a promulgação da Lei n. 12.737/12, a qual inclusive veio a ser apelidada de “Lei Carolina Dieckmann”.[99]

Se comparada aos diplomas que a antecederam, a referida legislação foi mais enfática na formulação de dispositivos diretamente relacionados à criminalidade cibernética. Dentre as inovações que trouxe ao texto do Código Penal, destaca-se a criação de um novo tipo penal, específico aos cibercrimes próprios, qual seja: “invasão de dispositivo informático”, que passou a ser previsto no artigo 154-A do CP.[100]

Conforme explica a doutrina, a conduta de copiar indevidamente dados ou informações eletrônicas não possuía, até então, uma previsão legal própria dentro do sistema penal brasileiro. Por este motivo, não era incomum que as

---

[98] BRASIL. **Projeto de Lei nº 2793, de 2011**. Disponível em: https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218.

[99] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 61.

[100] BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

autoridades se valessem de outros tipos penais, como o furto (art. 155, CP),[101] para promover a responsabilização nesses casos.[102]

Portanto, com a promulgação da Lei n. 12.737/12, introduziu-se na legislação pátria previsões mais específicas quanto à invasão desses dispositivos, permitindo que tais condutas sejam processadas sem novas violações aos princípios da legalidade e da vedação à analogia *em malam partem*.[103]

Optou-se por um artigo amplo, já que o caput e os parágrafos do referido artigo preveem a responsabilização para uma série de ilícitos relacionados às práticas de destruição, adulteração, apropriação, transmissão ou comercialização não autorizada de dados e informações digitais – ou seja, de condutas que, de algum modo, atentam contra a integridade desses conteúdos.[104]

Nesse sentido, incrimina-se não apenas a invasão de dispositivo informático alheio, mas também condutas que a ela são conexas, tais como a instalação de vulnerabilidades e a difusão de dispositivo ou programa que facilite tais ingressos não autorizados.

Cabe salientar que tal inovação legislativa foi vista com bons olhos pela doutrina especializada. Ainda que com algumas falhas, destaca-se que o referido artigo instituiu tratamento técnico-jurídico a toda uma gama de condutas delituosas, praticadas no âmbito das novas tecnologias, que costumavam ser negligenciadas pelas normas penais.

Ademais, considera-se positivo o fato de o texto legal ter adotado uma linguagem relativamente neutra, capaz de abarcar distintas formas de ataque a

---

[101] Inclusive esse foi o encaminhamento utilizado no caso do vazamento de fotos da atriz C. Dieckmann, conforme se verifica na reportagem “Polícia encontra hackers que roubaram fotos de Carolina Dieckmann”, vinculada ao portal de notícias G1. Disponível em: http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html.

[102] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 74.

[103] Idem.

[104] BUSATO, Paulo César. **Direito penal**: parte especial 1. – 2 ed. – São Paulo: Atlas, 2016, p. 402.

dispositivos tecnológicos variados – tais como computadores, smartphones e outros gadgets - estando eles conectados ou não à Internet. [105]

Entretanto, a opção do legislador em condensar variados ilícitos em um número reduzido de disposições parece ter se revelado problemática. Diversas são as ressalvas apontadas pela doutrina acerca do referido artigo, especialmente quanto às lacunas e os problemas práticos que decorrem de sua aplicação.

Primeiramente, quanto ao caput do artigo 154-A, CP,[106] ressalta-se que a expressão "invadir dispositivo informático alheio" afasta, de antemão, qualquer responsabilização ao indivíduo que invade e viola a integridade informacional de dispositivo próprio,[107] como nos casos de "destravamentos" e "jailbreaking" de aparelhos eletrônicos.[108]

De modo semelhante, autores entendem que tal expressão torna atípica a conduta do indivíduo que invade dispositivo próprio para obter, indevidamente, dados informáticos alheios[109]. Nas palavras Vianna e Machado:

> Em lan houses ou "cyber cafés", por exemplo, o proprietário dos dispositivos informáticos não praticará o crime se acessar sem autorização os dados do usuário que alugar a máquina. Da mesma forma, será atípica a conduta do empregador que acessar e-mails pessoais do empregado sem sua autorização armazenados em seu computador do trabalho.[110]

Diversas críticas também são formuladas quanto ao trecho "mediante violação indevida de mecanismo de segurança". Primeiramente, cabe destacar

---

[105] BRITO, Auriney. **Análise da Lei 12.737/12**: Lei Carolina Dieckmann, 2013. Disponível em: http://politicacidadaniaedignidade.blogspot.com/2013/04/analise-da-lei-1273712-lei-carolina.html.

[106] Assim dispõe o caput do artigo 154-A, CP: "Invadir dispositivo informático alheio, conectado ou não à 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 para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa". BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

[107] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 91.

[108] Tais infrações poderiam tão somente ser enquadradas na Lei dos Softwares (Lei 9609/98).

[109] Jesus e Milagre, de outro modo, entendem que a interpretação não poderia ser tão restritiva, de modo que o sujeito passivo poderia ser o titular dos dados e não apenas do dispositivo eletrônico. JESUS; MILAGRE, op. cit., p. 87.

[110] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 116.

que tal previsão gera sérias consequências práticas, haja vista que, em respeito ao princípio da legalidade, os dispositivos desprovidos de mecanismos de segurança (tais como pendrives e cartões de memória, por exemplo) não poderiam ser protegidos por esse artigo.[111]

Ademais, questiona-se a excessiva amplitude do termo, o qual não apresenta qualquer definição acerca de quais poderiam ser esses obstáculos - se apenas digitais ou também físicos – gerando dúvidas na interpretação do referido artigo.[112]

Também, é possível citar o embate na doutrina acerca da invasão para inserção de novas informações. Para alguns autores tal conduta seria atípica, por falta de previsão legal nesse sentido. Contudo, para outros, haveria responsabilização com base no núcleo do tipo “adulterar”.[113]

De mesmo modo, discute-se acerca da possibilidade de responsabilização daquele que invade dispositivo para tão somente analisar as informações, sem qualquer tipo de cópia de material. Tratar-se-ia de uma atipicidade ou a conduta estaria abarcada pelo verbo “obter”, em razão de o sujeito ter tido contato com o conteúdo? Os autores se dividem neste tópico.[114]

Destaca-se, porém, que as críticas não ficam restritas ao caput. O parágrafo 1º, por exemplo, é visto como um verdadeiro avanço nas barreiras de imputação, visto que criminaliza uma série de condutas prévias ao cometimento da efetiva invasão informática apenas com base no risco abstrato que estas poderiam causar à integridade desses dados e informações.[115]

Ademais, questiona-se a construção do legislador em relação às penalidades previstas no referido artigo, visto que a imprecisão da redação e a

---

[111] Jesus e Milagre consideram problemática tal disposição, nas palavras deles, “seria como se o legislador não punisse o furto de um carro que não possui alarme”. JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 88.

[112] Como exemplo prático, Jesus e Milagre propõem o caso de um pen drive guardado no interior de um cofre. Para o autor, haveria a incidência do artigo 154-A, CP, todavia, reconhece que não existe uma unanimidade na doutrina. Ibidem, p. 78.

[113] Ibidem, p. 90.

[114] Ibidem, p. 89.

[115] BUSATO, Paulo César. **Direito penal**: parte especial 1. – 2 ed. – São Paulo: Atlas, 2016, p. 406.

inadequada disposição das penas ao longo do texto podem acarretar em embaraços numa eventual dosimetria.[116]

Para além da inserção do supracitado tipo penal no ordenamento jurídico pátrio, a Lei n. 12.737/12 ainda realizou breves alterações em outras regras do Código Penal: tais como os artigos 266 e 298, conforme se passará a expor.

Mesmo com a inquestionável importância que os sistemas informáticos têm em nossa sociedade atual, a eles ainda não era garantida a mesma proteção jurídica despendida aos serviços telegráficos, radiotelegráficos e telefônicos.

Nesse sentido, inseriu-se o parágrafo primeiro ao artigo 266, CP, o qual passou a dispor da seguinte redação:

> **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
>
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de um a três anos, e multa.
>
> § 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.[117]

Por intermédio da criação desse novo parágrafo, a supracitada lei, de certo modo, equiparou os serviços telemáticos[118] aos demais meios de transmissão de informações, reconhecendo sua importância prática e protegendo-os contra interrupções criminosas.

Insta salientar que o legislador optou por excluir o verbo “perturbar” do âmbito dos serviços telemáticos, subsistindo somente responsabilização para

---

[116] BUSATO, Paulo César. **Direito penal**: parte especial 1. – 2 ed. – São Paulo: Atlas, 2016, p. 406.

[117] BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

[118] Jesus e Milagre entendem como serviços telemáticos o “conjunto de tecnologias de transmissão de dados que resultam da união de recursos de telecomunicações e da informática, e que permitem o processamento, a compressão, o armazenamento e a comunicação de dados”. JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 103.

as condutas que, de fato, interromperem a prestação de tais serviços.[119] Todavia, entende-se como pertinente tal opção legislativa, visto que diversas atividades lícitas – como farejamento de redes, rastreamento de host e comandos de ping – são capazes de provocar leves perturbações na rede, o que resultaria numa criminalização descabida desses atos.[120]

Porém, destaca-se que o referido artigo do Código Penal está inserido no rol dos crimes contra a incolumidade pública, razão pela qual apenas haveria a criminalização, nesse tipo penal, de condutas capazes de atingir uma quantidade indeterminada de pessoas.[121]

Sendo assim, para ataques individualizados, visando o prejuízo de sistemas específicos, estaria afastada a incidência dessas disposições, restando apenas a responsabilização com base no crime de dano (art. 163, CP) ou de violação da comunicação (art. 151, §1º, III, CP).[122]

De modo similar à proteção dos serviços telemáticos, a Lei n. 12.737/12 buscou realizar uma modernização no tipo penal referente à falsificação de documento particular. Assim, adicionou-se um parágrafo único ao artigo 298, CP, cuja redação determina a inclusão dos cartões pessoais, de crédito e de débito, à categoria de “documento particular”:

> **Falsificação de documento particular**
>
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> **Falsificação de cartão**
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.[123]

---

[119] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p.130.
[120] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 106.
[121] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013, p. 130.
[122] JESUS; MILAGRE, op. cit., p. 107.
[123] BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

O tratamento jurídico conferido ao tipo penal permanece o mesmo, ocorrendo tão somente a adição de novos objetos materiais[124] ao conceito cunhado no caput. Segundo a doutrina, tal modificação teria sido justificada pelo aumento no número de fraudes bancárias envolvendo a clonagem dos referidos cartões.[125]

Apesar disso, entende-se que a inovação trazida pelo parágrafo único do art. 298, CP foi demasiado simplória, visto que se perdeu a oportunidade de equiparar outros documentos físicos e eletrônicos à categoria de documento particular, tal como o certificado digital.[126]

Além do mais, resgata-se que, em respeito ao princípio da legalidade, resta vedada a aplicação do referido dispositivo para casos outros do que a mera clonagem física dos cartões.[127] Nesse sentido, a despeito das contribuições que a presente alteração legislativa trouxe quanto às fraudes bancárias, é mister reconhecer que os ganhos foram aquém do que poderiam ter sido, subsistindo lacunas jurídicas para diversas práticas criminosas.[128]

Desse modo, apesar da Lei n. 12.737/12 ter contribuído de maneira substancial a um adequado enfrentamento da temática, verifica-se que ainda subsistem falhas e lacunas a serem dirimidas.

E, nesse contexto de busca por uma maior regulamentação do uso da Internet, exsugiu o Marco Civil da Internet no ano de 2014, o qual foi desenvolvido através de um diálogo amplo entre a sociedade civil e o Poder Público.

2.3 “MARCO CIVIL DA INTERNET” (Lei n. 12.965/14).

A Lei n. 12.956/14, popularmente conhecida como Marco Civil da Internet, nasceu com o intuito de ser uma “Constituição da Internet”, positivando direitos e deveres a todos os atores relacionados à rede mundial de

---

[124] BUSATO, Paulo César. **Direito penal**: parte especial 2, v.3. – São Paulo: Atlas, 2017, p. 373.
[125] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 110.
[126] Ibidem, p.114.
[127] Ibidem, p.113.
[128] Segundo Jesus e Milagre, trata-se de uma disposição que “já nasce com lacunas e com prazo de validade atrelado à evolução tecnológica”. Ibidem, p. 114.

computadores – usuários, empresas de telecomunicação e o próprio Estado.[129] Prestou importante papel na formulação de uma base teórica às relações digitais, regulamentando o uso da Internet no Brasil e garantindo sua fruição condizente com os ditames da Constituição Federal de 1988.[130]

Fruto de uma parceria entre a Secretaria de Assuntos Legislativos do Ministério da Justiça e o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (Rio de Janeiro), o Marco Civil caracterizou-se por ser uma construção colaborativa e democrática, com a participação de diversos setores da sociedade civil, por intermédio de consultas públicas disponibilizadas na própria Internet. [131]

Diversos foram os eventos, conferências, audiências e seminários realizados no processo de elaboração do texto definitivo. Nesse sentido, destaca-se o caráter democrático do referido diploma legislativo, pois criou um rico ambiente de diálogo entre o Estado e a sociedade civil, particularmente na tratativa dos temas mais sensíveis ao projeto.[132]

A referida Lei é subdividida em cinco capítulos. Destaca-se o primeiro, o qual elenca os fundamentos, princípios e objetivos a serem observados na utilização da Internet no Brasil.[133]

Dentre os fundamentos, o artigo 2º elenca o respeito aos direitos humanos e à liberdade de expressão, o estímulo ao desenvolvimento da personalidade e da cidadania em meios digitais e a valorização da pluralidade e diversidade, em consonância com a finalidade social da rede[134].

Quanto aos princípios, o artigo 3º do Marco Civil ressalta, entre outros, a garantia da liberdade de expressão e manifestação de pensamento, proteção

---

[129] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p.166.

[130] SANTOS, Vinicius Wagner Oliveira. **Neutralidade da rede e o Marco Civil da Internet no Brasil**: atores, políticas e controvérsias. 2016. Tese (Doutorado em Direito) - Universidade Estadual de Campinas, Campinas, p. 148-149. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/321453/1/Santos_ViniciusWagnerOliveira_D.pdf.

[131] JESUS; MILAGRE, op. cit., p. 166.

[132] SOUZA, João Éder Furlan Ferreira de. **Desigualdade digital no Brasil**: Desafios jurídico-políticos para uma sociedade informacional inclusiva. Dissertação de mestrado. Programa de Pós-Graduação em Ciência Jurídica, Universidade Estadual do Norte do Paraná, Jacarezinho, 2017, p. 120. Disponível em: https://uenp.edu.br/pos-direito-teses-dissertacoes-defendidas/direito-dissertacoes/9681-joao-eder-furlan-ferreira-de-souza/file.

[133] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[134] Idem.

da privacidade dos usuários, preservação da estabilidade, segurança e neutralidade de rede, bem como o estímulo ao uso de boas práticas, inclusive com a responsabilização dos agentes de acordo com suas atividades.[135]

Em consonância com as disposições anteriores, o artigo 4º elenca os principais objetivos do Marco Civil da Internet, dentre os quais ressaltam-se a promoção do acesso universal à internet e o fomento à difusão de novas tecnologias, com vistas a promover a comunicação e a acessibilidade.[136]

O terceiro capítulo, por sua vez, apresenta uma abordagem mais voltada aos serviços de fornecimento de Internet e às suas aplicações. Para tanto, subdivide-se em quatro seções principais, relativas à neutralidade da rede, proteção às informações e dados privados, requisição judicial de registros, bem como a responsabilidade dos provedores por danos decorrentes do conteúdo de terceiros, a qual será analisada de maneira pormenorizada no capítulo subsequente.[137]

A respeito desses temas, destaca-se o artigo 9º - um dos pilares do Marco Civil da Internet - o qual impõe o estrito respeito à neutralidade da rede.[138] Nos seus termos, "o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação", de forma a impedir diferenciações entre os usuários, baseadas no material que eles acessam na rede.[139]

De mesmo modo, a Lei n. 12.965/14 introduziu no ordenamento jurídico brasileiro expressivas disposições acerca da obrigação dos prestadores de Internet em manter registros de conexão de seus clientes à rede.[140] Antes da promulgação do Marco Civil, cabe destacar, existia apenas uma recomendação

---

[135] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
[136] Idem.
[137] Idem.
[138] SANTOS, Vinicius Wagner Oliveira. **Neutralidade da rede e o Marco Civil da Internet no Brasil**: atores, políticas e controvérsias. 2016. Tese (Doutorado em Direito) - Universidade Estadual de Campinas, Campinas, p. 204-205. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/321453/1/Santos_ViniciusWagnerOliveira_D.pdf.
[139] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
[140] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 170.

por parte do Comitê Gestor Internet Brasil para que tais provedores (de acesso) mantivessem, pelo prazo de três anos, “dados de conexão e comunicação realizadas por seus equipamentos (identificação do endereço IP, data e hora de início e término da conexão e origem da chamada)”.[141]

Com o advento da referida lei, instituiu-se o dever de os provedores de acesso manterem os registros de conexão dos usuários pelo prazo mínimo de um ano.[142] Ademais, o artigo 15 do Marco Civil estendeu tal exigência também aos provedores de aplicações ou serviços, obrigando-os a manterem tais registros pelo prazo mínimo de seis meses,[143] de modo a facilitar a cooperação desses agentes privados na investigação de eventuais crimes.

Entretanto, por mais relevantes que possam ser tais registros às investigações policiais, em razão dos direitos à inviolabilidade e ao sigilo de navegações e comunicações na rede,[144] impôs-se a necessidade de ordem judicial para o acesso a esses dados de conexão,[145] mesmo que o requerimento parta das autoridades competentes - situação que causa debates na doutrina.[146]

Em síntese, o Marco Civil destacou-se por ser uma lei inovadora na forma de regulamentar a utilização da Internet no Brasil. Ao invés de ter sido

---

[141] Ponto 3.2 das “Recomendações para o desenvolvimento e operação da Internet no Brasil”. Disponível em: https://www.cg.org.br/recomendacoes-para-o-desenvolvimento-e-operacao-da-internet-no-brasil.

[142] Artigo 13, caput, Lei n. 12.965/14: “Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento”. BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[143] Artigo 13, caput da referida lei: “O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento”. Idem.

[144] De acordo com o Artigo 7º do Marco Civil: “O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos”:
“II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial”. Idem.

[145] Ressalta-se que os registros de conexão não se confundem com os dados cadastrais do usuário - tais como filiação, o endereço e a qualificação pessoal - os quais podem ser acessados pelas autoridades sem ordem judicial. BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev., p. 43. - Brasília: MPF/2ªCCR, 2013. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

[146] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 172-173.

desenvolvida puramente como uma lei criminal, tipificando condutas consideradas nocivas no âmbito informático, priorizou-se por adotar uma legislação mais “principiológica”, uma espécie de “carta de intenções”, com foco nos direitos, fundamentos e objetivos a serem alcançados no uso da Rede.[147]

A despeito de algumas polêmicas e críticas que o circundam, considera-se inegável a contribuição do referido diploma para a definição dos alicerces a serem seguidos no desenvolvimento da Internet e de outras tecnologias que lhes são conexas. Porém, por mais benéfico que seja, é preciso destacar que o Marco Civil não foi capaz de solucionar integralmente as lacunas presentes no sistema, em especial no âmbito dos crimes cibernéticos, haja vista que poucas foram as disposições práticas nesse sentido.[148]

Dessa forma, a criminalidade cibernética continua a fazer parte da pauta do Poder Legislativo, com discussão frequente de projetos sobre a temática, tais como o PL n. 5452/16,[149] o qual culminou com a promulgação da Lei n. 13.718/18, que, dentre suas tratativas, dispõe sobre a utilização dos sistemas informáticos na prática de crimes sexuais.

2.4 LEI N. 13.718/18

A Lei n. 13.718/2018 foi promulgada com o intuito de reforçar a punição aplicada a crimes cometidos contra a dignidade sexual, com especial enfoque no combate ao estupro e à importunação sexual.[150]

Cabe destacar que as primeiras negociações acerca do referido diploma possuíam um caráter bem mais restritivo, seu primeiro projeto - o PLS n.

---

[147] SANTOS, Vinicius Wagner Oliveira. **Neutralidade da rede e o Marco Civil da Internet no Brasil**: atores, políticas e controvérsias. 2016. Tese (Doutorado em Direito) - Universidade Estadual de Campinas, Campinas, p. 144-145. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/321453/1/Santos_ViniciusWagnerOliveira_D.pdf.

[148] WERLE, Vera Maria; OLIVEIRA, Bruna Machado de; MATTOS, Karoline Reis; SIQUEIRA, Marcela Scheuer. **Crimes virtuais e a legislação brasileira**. (Re) Pensando Direito, EDIESA, Ano 7, n. 13, jan./jun., 2017, p. 128-129. Disponível em: http://local.cnecsan.edu.br/revista/index. php/direito/article/viewFile/468/342.

[149] BRASIL. **Projeto de Lei n. 5452, de 2016**. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra; jsessionid=A24E46AE366969B7F42D0D5449FF6258.proposicoesWebExterno2?codteor=1630876&filename=Avulso+-PL+5452/2016.

[150] Idem.

618/15[151] - tratava apenas da criação de novas causas de aumento de pena para o crime de estupro, nas hipóteses em que este era cometido em concurso de agentes.[152] Apenas com o passar dos anos é que o texto passou a englobar outras previsões, assemelhando-se àquele promulgado em 24 de setembro de 2018.

Sua redação definitiva, portanto, previu diversas alterações no texto do Código Penal brasileiro, especificamente em seu Título VI.[153] Dentre elas, alterou-se para pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual, estipularam-se novas causas de aumento de pena para alguns desses delitos, bem como houve a criação de novos tipos penais, quais sejam - a supracitada - importunação sexual e a divulgação de cena de estupro, sexo ou nudez.[154]

Em relação a esta última disposição, optou-se por criminalizar condutas como as de oferecer, divulgar, vender registro audiovisual que contenha cena de sexo ou nudez, de maneira não autorizada pela vítima, bem como de estupro.[155] Assim restou previsto o caput do artigo 218-C do CP:

> **Art. 218-C:** Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.

---

[151] BRASIL. **Projeto de Lei n. 5452, de 2016**. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A24E46AE366969B7F42D0D5449FF6258.proposicoesWebExterno2?codteor=1630876&filename=Avulso+-PL+5452/2016.

[152] BARRETO, Alessandro Gonçalves; BARRETO, Karolinne Brasil. **Lei 13.718/18**: criminalização da divulgação de cena de sexo, nudez e pornografia sem consentimento da vítima e outros delitos. Disponível em: https://www.migalhas.com.br/dePeso/16,MI288717,81042-Lei+1371818+criminalizacao+da+divulgacao+de+cena+de+sexo+nudez+e.

[153] BRASIL. **Lei 13.718/2018,** de 24 de setembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm.

[154] CUNHA, Rogério Sanches. **Lei 13.718/18:** Introduz modificações nos crimes contra a dignidade sexual. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2018/09/25/lei-13-71818-introduz-modificacoes-nos-crimes-contra-dignidade-sexual.

[155] OLIVEIRA, Marcel Gomes. **As inovações legislativas aos crimes sexuais no enfrentamento à criminalidade**: comentários à lei n. 13.718/18. Disponível em: http://emporiododireito.com.br/leitura/as-inovacoes-legislativas-aos-crimes-sexuais-no-enfrentamento-a-criminalidade-comentarios-a-lei-n-13-718-2018.

> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Desse modo, verifica-se a pertinência do dispositivo legal à temática dos crimes cibernéticos, haja vista a previsão de utilização das novas tecnologias, quais sejam os sistemas de informática ou telemática, como um dos possíveis meios de perpetração do delito.

Tal relevância é ainda mais acentuada quando da análise do parágrafo 1º do referido artigo, o qual institui uma causa de aumento de pena para os casos em que o autor do crime mantenha ou tenha mantido relação íntima de afeto com a vítima, ou então que tenha a intenção de humilhá-la - clara referência do legislador às práticas de “revenge porn”, nas quais devassa-se publicamente a intimidade de outrem sob pretexto de ridicularização ou vingança, por exemplo.[156]

Ainda que sucintas, tais disposições se revelam de grande importância para uma regulamentação jurídica mais adequada acerca dessa criminalidade cibernética, visto que auxiliam na diminuição das lacunas de punibilidade que ainda perduram para alguns desses crimes.[157]

Nesse sentido, destaca-se, inclusive, a possibilidade do referido dispositivo legal ser aplicado em concurso com o artigo 154-A, CP, de modo a permitir uma persecução mais robusta para casos similares àquele enfrentado pela atriz Carolina Dieckmann.[158]

Diante de todo o exposto, a respeito da produção legislativa construída aos longos dos anos, aparenta-se ser possível tecer algumas considerações sobre o panorama legislativo brasileiro, no que tange a seus aspectos positivos e negativos.

Primeiramente, é possível destacar que as inovações legislativas foram importantes no desenvolvimento de uma regulamentação jurídica mais

---

[156] Assim dispõe o parágrafo 1º do artigo 218-C, CP: “§ 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação”. BRASIL. **Lei 13.718/2018,** de 24 de setembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm.

[157] OLIVEIRA, Marcel Gomes. **As inovações legislativas aos crimes sexuais no enfrentamento à criminalidade**: comentários à lei n. 13.718/18. Disponível em: http://emporiododireito.com.br/leitura/as-inovacoes-legislativas-aos-crimes-sexuais-no-enfrentamento-a-criminalidade-comentarios-a-lei-n-13-718-2018.

[158] Idem.

adequada ao enfrentamento desses delitos. Mediante o estudo dos diplomas citados, constata-se a ocorrência de um “amadurecimento” por parte do legislador, no sentido de reconhecer a existência de particularidades nessa nova criminalidade e buscar maneiras diferenciadas de se solucionar os problemas.

Cabe ressaltar, ademais, que as leis promulgadas passaram a adotar um tom mais neutro, se distanciando dos discursos mais radicais e incriminadores presentes nos primeiros projetos de lei sobre a temática.

De todo modo, por mais que tenha havido um aprimoramento no trato da criminalidade cibernética, a doutrina é clara ao apontar a subsistência de lacunas e problemas nos dispositivos legais mencionados.[159]

Nesse sentido, destaca-se a importância da busca constante pelo aperfeiçoamento dos instrumentos de persecução desses delitos, inclusive mediante a cooperação entre agentes públicos e privados. Por tal razão, o presente trabalho buscará analisar, de modo mais exaustivo, aspectos relacionados à participação dos provedores de Internet no bojo das investigações, atentando-se, inclusive, à possibilidade responsabilização de tais agentes.

[159] Inclusive por conta da forma como tais leis foram promulgadas, de maneira apressada e baseada em casuísmos. JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016, p. 62.

3 CRIMES CIBERNÉTICOS SOB AS PERSPECTIVAS DA INVESTIGAÇÃO E DA RESPONSABILIZAÇÃO DOS PROVEDORES

A produção tecnológica é profundamente marcada pelo dinamismo e mutabilidade, inovações surgem e se sobrepõem numa velocidade cada vez mais crescente.[160] Porém, conforme exposto, tais atributos são também apropriados pela criminalidade, a qual se vale dos meios informáticos para aperfeiçoar e desenvolver novas práticas ilícitas.

Em complemento, ressalta-se que a inovação tecnológica, quando utilizada para a prática de infrações, tende a gerar sensíveis complicações à atuação das autoridades policiais, haja vista a dificuldade de se coletar provas e determinar a autoria em muitos desses delitos.[161]

Nesse sentido, de modo a conter o crescimento da criminalidade cibernética e sua engenhosidade característica, tem-se como imprescindível o constante aperfeiçoamento dos agentes, aliado ao aprimoramento da estrutura forense, com vistas a proporcionar uma adequada investigação dos casos.[162]

Entretanto, é preciso destacar que o enfrentamento dos cibercrimes não pode se limitar somente ao aprimoramento das estruturas tradicionais de persecução criminal. De modo diverso, defende-se a busca por soluções originais, relacionadas, muitas vezes, à cooperação entre setores públicos e privados – como no fornecimento, pelos provedores de Internet, de informações necessárias às investigações.[163]

Conforme destaca Soares:

---

[160] BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017, p. 52. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.

[161] Ibidem, p. 19.

[162] SEGER, Alexander. **Cybercrime Training for Judges**: training manual. – Strasbourg: Economic Crime Division, Council of Europe, 2010, p. 67. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventos-internacionais/conteudo-banners-1/crimes-ciberneticos/cybercrime-training-for-judges-training-manual/view.

[163] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 388.. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

> A criatividade, o dinamismo e a inovação caracterizam o fenômeno criminoso. Por isso, a repressão estatal também necessita ser criativa dinâmica e inovadora, com uma importante diferença: a ação criminosa é absolutamente livre, enquanto a repressão estatal é fortemente condicionada pelo ordenamento jurídico, especialmente pelos direitos fundamentais.[164]

No tocante aos provedores, o Marco Civil instituiu expressamente o dever de conservação temporária dos registros informáticos dos usuários, de modo a facilitar a colaboração com a Justiça em eventuais investigações. Todavia, a despeito desta clara previsão, persistem algumas controvérsias acerca da aplicação prática dessas disposições, precipuamente no que se refere aos efeitos criminais.

Assim sendo, o presente capítulo se propõe a realizar uma análise das peculiaridades do processo de investigação dos crimes cibernéticos, com especial enfoque sobre a participação dos provedores de Internet nesse processo, sem desconsiderar, contudo, as possibilidades de responsabilização que estes podem sofrer no descumprimento das exigências legais.

3.1 PECULIARIDADES DA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

No atual contexto, de uma sociedade marcada por inovações e riscos derivados da expansão tecnológica, verifica-se uma extensa difusão dos aparatos informáticos ao longo do corpo social, bem como uma crescente preocupação com a integridade desses dados e sistemas.

Com vistas a proteger tais anseios, passou-se a requerer das autoridades policiais uma expertise também acerca dessas inovações tecnológicas, fazendo-se necessário uma atualização e uma crescente especialização de seus profissionais no trato com essas questões.[165]

---

[164] SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**: perspectivas e limites. Tese de doutorado. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014, p. 206. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2137/tde-30112015-165420/pt-br.php.

[165] BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017, p. 35. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.

Como não poderia deixar de ser, os crimes cibernéticos se revelam naturalmente dinâmicos, inventivos nos modos de utilização da informática na prática dos mais diversos ilícitos. De mesmo modo, portanto, exige-se que assim seja a atuação das estruturas de persecução criminal – pautada numa lógica de constante aprendizado e aprimoramento.[166]

Ressalta-se que o atual panorama tecnológico possibilita o acesso à Internet por meio dos mais diversos dispositivos eletrônicos – desde os tradicionais computadores, até smartphones, eletrodomésticos e carros.[167] Por tais motivos, resta notória a necessidade de que as investigações criminais sejam feitas de maneira diligente, tomando em conta as particularidades dos instrumentos utilizados na prática delitiva.[168]

Em decorrência da pluralidade desses instrumentos, destaca-se que diversificada também pode ser a produção probatória no bojo das investigações de crimes cibernéticos: arquivos digitais, cookies, históricos de navegação, e-mails e registros de servidores são exemplos de informações que podem ser utilizadas para a elucidação dos casos.[169]

De todo modo, entende-se que as tais evidências digitais poderiam ser estudadas de maneira conjunta, tendo em vista as especialidades que possuem frente aquelas derivadas de crimes tradicionais.[170]

Em razão de estarem intimamente relacionadas ao meio digital, a doutrina acentua, em primeiro lugar, a fragilidade característica dessas evidências. De acordo com Seger, não se exigem maiores esforços para que

---

[166] BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017, p. 29. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.

[167] Ibidem, p. 28.

[168] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 369. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

[169] BRASIL, op. cit., p. 23.

[170] Evidência digital pode ser conceituada como toda informação guardada ou transmitida por meio de tecnologias informáticas, que pode dar suporte a uma linha investigativa. SEGER, Alexander. **Cybercrime Training for Judges**: training manual. – Strasbourg: Economic Crime Division, Council of Europe, 2010, p. 66. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventos-internacionais/conteudo-banners-1/crimes-ciberneticos/cybercrime-training-for-judges-training-manual/view.

elas venham a ser danificadas ou perdidas,[171] até mesmo durante os processos de coleta e valoração.[172]

De modo semelhante, ressalta-se o alto grau de volatilidade das evidências digitais, as quais podem ser facilmente modificadas, tanto pelo criminoso – na tentativa de ocultar seus rastros – quanto pelas próprias autoridades, se não adotados os cuidados necessários ao seu manuseio.[173]

Dentre outras características, ainda é possível destacar a facilidade de proliferação e multiplicação dessas informações, razões pelas quais se sugere a adoção de técnicas sofisticadas de filtragem durante a análise dos dispositivos investigados, de modo a minimizar os custos e maximizar a eficiência do trabalho realizado.[174]

Com base nas particularidades expostas, compreende-se a necessidade de a investigação dos crimes cibernéticos ser feita de modo minucioso, muitas vezes com a presença de profissionais especializados, capazes de dar o devido tratamento a essas evidências digitais.[175]

Nesse sentido, Wendt e Jorge ressaltam que tais investigações costumam se valer de duas fases distintas – uma fase técnica e outra fase de "campo" – havendo na primeira delas a realização de diversas diligências prévias à atuação policial *in loco*, com o intuito final de identificar o meio utilizado para a prática criminosa, bem como a localização física do instrumento que deu causa ao ilícito. [176]

Como dito, na etapa técnica são executadas uma série de tarefas e procedimentos investigativos, tais como: análise das informações prestadas pela vítima, formalização da ocorrência por meio de um registro ou boletim de

---

[171] A título de exemplo, o autor cita as informações contidas na memória RAM dos dispositivos, para quais se necessita da utilização de procedimentos técnicos específicos, sob risco de elas serem corrompidas com o desligamento do aparelho. Ibidem, p. 67.
[172] Idem.
[173] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 172. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.
[174] Ibidem, p. 173.
[175] BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017, p. 52. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.
[176] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013, p. 67.

ocorrência, investigação inicial acerca dos prováveis autores, identificação do dispositivo utilizado e, enfim, a solicitação da autorização judicial de quebra dos dados de acesso dos investigados à rede.[177]

A obtenção desses registros é uma etapa fundamental para a elucidação dos delitos, haja vista que, a partir deles, torna-se possível ter acesso aos "log" de conexão e de acesso do indivíduo na Internet, ou seja, ao conjunto de informações relativas à forma como ele se utilizou da rede - vide data, horário, fuso horário, tempo de conexão e o protocolo de Internet (IP).[178]

Nesse sentido, os autores ressaltam que é:

> Necessário trazer à baila a observação técnica de que, quando ocorre a conexão de um computador ou dispositivo similar à internet (como celular, tablete etc.) o endereço de IP (Internet Protocol) é atribuído exclusivamente para aquele internauta. Da mesma forma que dois corpos não ocupam o mesmo lugar no espaço, não existem dois usuários com o mesmo IP durante a navegação na internet [...].[179]

Porém, além de exclusivo, o IP também é dinâmico, visto que com o término da conexão de determinado usuário à rede, o protocolo até então conferido a ele torna-se novamente disponível, podendo ser repassado para outro internauta.

Desse modo, verifica-se que o IP, em si mesmo, não é capaz de auxiliar substancialmente a investigação, visto que a cada acesso o investigado possuirá um protocolo distinto, além de que "dado endereço de IP poder estar associado a centenas ou milhares de diferentes usuários por um período de semanas ou meses".[180]

Nesse sentido, destaca-se a importância da cooperação entre as autoridades policiais e os provedores de Internet na elucidação desses crimes cibernéticos, visto que apenas mediante o acesso aos registros desses provedores é que se possibilita a vinculação do número de IP a determinado

---

[177] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013, p. 68.
[178] Ibidem, p. 247-248.
[179] Ibidem, p. 68.
[180] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 383. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

investigado, particularizando qual o dispositivo informático vinculado a tal protocolo em certo dia e hora.[181]

Portanto, antes que a autoridade policial possa se valer de diligências presenciais – a denominada “fase de campo” - com eventual utilização da busca e apreensão sobre os dispositivos do suspeito, impõe-se a realização dessa investigação prévia, especializada, pautada na coleta de informações presentes na própria Internet e nos registros de seus provedores.

Assim sendo, em atenção às especificidades do processo investigativo dos cibercrimes, revela-se ser indispensável a busca por um constante aprimoramento pessoal e instrumental por parte das autoridades persecutórias. Porém, a dinamicidade das evidências digitais impõe que tal desenvolvimento também se valha de um diálogo mais próximo com os agentes privados, especialmente os provedores.

3.2 ANÁLISE DA RESPONSABILIZAÇÃO DOS PROVEDORES A PARTIR DO MARCO CIVIL DA INTERNET

Como visto, os provedores de internet desempenham papel fundamental no bojo das investigações acerca dos crimes cibernéticos, sua cooperação se faz muito relevante na obtenção de informações mais precisas acerca das atividades desempenhadas pelos usuários na utilização da Rede.

Nesse sentido, por exemplo, a Lei n. 12.965/14 (Marco Civil da Internet) inovou na ordem jurídica brasileira ao instituir um prazo mínimo para que os provedores retenham os registros de acesso à Internet e às suas aplicações – 01 ano[182] e 06 meses[183], respectivamente.

---

[181] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 383. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

[182] Artigo 13, Lei n. 12.965/14: “Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento”. BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[183] Artigo 15, Lei n. 12.965/14: “O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do

De todo modo, compreende-se que tais agentes privados não podem ter a colaboração restrita ao repasse dessas informações, visando a individualização do autor da infração. Ao contrário, entende-se que eles devem também participar ativamente, como por exemplo, através da retirada de conteúdos ilícitos contidos em suas páginas virtuais.[184]

Tal posicionamento também passou a dispor de fundamentação legal, visto que, na redação final do Marco Civil, incorporaram-se previsões acerca da possibilidade de os provedores – particularmente, de aplicações de Internet - serem subsidiariamente responsabilizados por danos decorrentes de conteúdos gerados por terceiros.

Porém, antes de adentrar de maneira mais específica a tais disposições, revela-se pertinente dispor de forma mais detalhada acerca dos tipos de provedores existentes no âmbito da Internet e das novas tecnologias, com o intuito de facilitar a compreensão do tema e delimitar, de modo mais preciso, quais as possibilidades de responsabilização cabíveis a esses agentes privados.

A Internet, a despeito de ter desenvolvido um vasto ciberespaço internacional, um ambiente de promoção do contato virtual entre usuários dos mais variados locais do globo, caracteriza-se por ser, em grande medida, uma rede física de transmissão de dados - atualmente, cada vez mais intrincada e ramificada - para qual se exige uma robusta infraestrutura de cabos, servidores, satélites e outros dispositivos tecnológicos.[185]

Devido à complexidade operacional que a Internet apresenta, revela-se natural o desenvolvimento de um robusto quadro mercantil conexo a essa tecnologia. Nesse sentido, é possível destacar a existência de um vasto contingente de agentes privados diretamente relacionados à manutenção, gestão, expansão e profusão desse mercado nas mais diversas localidades.

---

regulamento". **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[184] BARRETO, Alessandro Gonçalves; BARRETO, Karolinne Brasil. **Lei 13.718/18**: criminalização da divulgação de cena de sexo, nudez e pornografia sem consentimento da vítima e outros delitos. Disponível em: https://www.migalhas.com.br/dePeso/16,MI288717,81042 Lei+1371818+criminalizacao+da+divulgacao+de+cena+de+sexo+nudez+e.

[185] ROSA, Giovanni Santa. **Na era do wi-fi, a internet ainda depende de cabos para existir**. Disponível em: https://tecnologia.uol.com.br/noticias/redacao/2018/03/18/na-era-do-wi-fi-a-internet-ainda-depende-de-cabos-para-existir.htm.

Assim sendo, entende-se que terminologia “provedores de Internet” seria bastante ampla, capaz de abarcar variados ramos de atuação dessas empresas. Tratar-se-ia de um verdadeiro gênero, do qual decorreriam espécies de atividades, desde as mais estruturais ao funcionamento da Rede até aquelas que estão em contato próximo com o público consumidor.[186]

A respeito dessas espécies, em primeiro lugar é cabível tratar sobre os denominados Provedores de Backbone, quais sejam os agentes privados vinculados ao aprimoramento das “fundações” da Internet, ao desenvolvimento de sua “espinha dorsal”.[187] São empresas de infraestrutura, que vendem a outros agentes econômicos o acesso a suas tecnologias de transmissão e sustentação do tráfego informático – estando, a princípio, alheias ao armazenamento de dados e à criação de conteúdos na Rede.[188]

Em contato direto com estes, estão os Provedores de Acesso, empresas que se valem da estrutura constituída pelos backbones, com vistas a oferecer o serviço de acesso à Internet para os usuários. Atuam, portanto, como intermediários, proporcionando a conexão entre o dispositivo do consumidor e as estruturas basilares ao funcionamento da web.[189]

Derivados do acesso à Internet, sobressaem-se outras espécies de provedores, relacionados a toda uma gama de produtos e aplicações ofertadas ao público. Dentre eles, existem os Provedores de Correio Eletrônico, os quais fornecem acesso a um sistema de armazenamento e transmissão de mensagens eletrônicas, personalizado em contas únicas, com utilização de login e senha para cada um desses usuários de e-mail.[190]

---

[186] Nesse sentido, compreende-se provedor de internet como sendo “todo aquele que viabiliza, de modo direto ou indireto, meios materiais hábeis a manter os indivíduos conectados à rede mundial de computadores”. COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da internet. Revista dos Tribunais, vol. 957, julho de 2015, p. 06. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

[187] No mercado brasileiro, destacam-se as seguintes empresas: Embratel, Global Crossing, Brasil Telecom, Telecom Italia e a Rede Nacional de Ensino e Pesquisa (RNP). Conforme relata a reportagem “O que é backbone”, vinculada no portal Canaltech. Disponível em: https://canaltech.com.br/telecom/o-que-e-backbone.

[188] COLAÇO, op. cit., p. 04.

[189] Idem.

[190] COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da internet. Revista dos Tribunais, vol. 957, julho de 2015, p. 05. Disponível em:

De modo semelhante, os Provedores de Hospedagem são empresas que fornecem o armazenamento de dados informáticos em servidores de acesso remoto, permitindo que o usuário e terceiros, previamente determinados, detenham a possibilidade de visualizá-los. Trata-se de um "contrato de cessão de espaço em disco rígido" muito comum atualmente, ocorrido tanto na criação de perfis nas redes sociais, quanto no desenvolvimento de sites próprios na Rede.[191]

Por fim, destacam-se os Provedores de Conteúdo, agentes relacionados à efetiva produção e divulgação de materiais criados na Internet. Trata-se de uma espécie bastante ampla, composta tanto de pessoas físicas como jurídicas, as quais são capazes de desenvolver novos conteúdos digitais, disponibilizá-los na Rede, ou então indicar seu acesso,[192] como nos casos dos sites de busca.[193]

Muitas das categorias apresentadas costumam se confundir na prática de mercado - é possível que provedores de backbone sejam também de acesso, que provedores de acessos disponibilizem de serviços de e-mail, também que aqueles de hospedagem sejam também provedores de conteúdo, dentre outras possibilidades – mas, seja como for, entende-se que a relevância teórica subsiste, de modo a facilitar a compreensão sobre as possibilidades de responsabilização aos agentes privados previstas no ordenamento jurídico pátrio.

Os provedores de backbone, por exemplo, poderão responder civilmente pela falha na prestação de seus serviços, defeitos em seus programas e equipamentos, até mesmo pela violação à livre concorrência,[194] na hipótese de

---

http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

[191] ANDRIGHI, Fátima Nancy. **A responsabilidade civil dos provedores de pesquisa via Internet**. Rev. TST. vol. 78, n. 3, jul./set., São Paulo, 2012, p. 65. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=3.

[192] Ibidem, p. 66.

[193] COSTA, Thabata Filizola. **Como era e como é a responsabilidade civil dos provedores de Internet no Brasil?** Mudanças trazidas pelo marco civil da Internet. Disponível em: https://thabatafc.jusbrasil.com.br/artigos/316058731/como-era-e-como-e-a-responsabilidade-civil-dos-provedores-de-internet-no-brasil.

[194] Valor previsto expressamente na Lei n. 12.965/14, em seu artigo 2º, V: "a disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: a livre iniciativa, a livre concorrência e a defesa do consumidor". BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

ter favorecido ou prejudicado indevidamente a algum provedor de acesso em relação aos seus pares.

No entanto, destaca-se que a relação dessas empresas com o público em geral é mínima, dificilmente havendo possibilidade de configuração de uma relação de consumo na utilização de suas estruturas. Sendo assim, considerando seu caráter mais basilar, entende-se como incabível a responsabilização desses provedores em razão de ilícitos praticados por terceiro usuário de conexão com a Internet.[195]

Nestes termos, Colaço manifesta-se no sentido de que:

> Diante disso, reforça-se o entendimento de que empresa prestadora de serviço de "espinha dorsal" da Internet não pode ser responsabilizada por ilícitos não praticados diretamente, pois sua função é fornecer a estrutura técnica sem a qual as informações editadas por terceiros não chegariam ao ciberespaço. Também não é possível exigir, dos provedores em epígrafe, identificação e localização de usuários de provedores de acesso e hospedagem, mas tão somente a identificação destes provedores.[196]

Os provedores de acesso, por sua vez, encontram-se mais próximos do grande público, estabelecendo verdadeiras relações consumeristas, com vistas a possibilitar o acesso dos usuários e outros agentes privados à web.[197]

De mesmo modo, podem vir a ser civilmente responsabilizados em razão das falhas no cumprimento dos contratos e da insatisfação com o desenvolvimento dos serviços prestados. Porém, em razão de se restringirem ao fornecimento da conexão à Internet, não possuiriam regência sobre os conteúdos disponibilizados na Rede, podendo apenas serem convocados a impedir a visualização de determinadas matérias, mediante expressa ordem judicial.[198]

Ainda, quanto aos seus deveres perante a Justiça, é preciso relembrar da necessária colaboração desses agentes privados com as investigações criminais, através do repasse dos registros de conexão dos usuários em caso

---

[195] COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da internet. Revista dos Tribunais, vol. 957, julho de 2015, p. 06. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

[196] Idem.

[197] Idem.

[198] Ibidem, p. 07.

de requisição judicial. Do descumprimento dessas disposições pode decorrer alguma sorte de penalização,[199] conforme indica o artigo 13, § 6º do Marco Civil.[200]

Em relação aos provedores de correio eletrônico, em razão de prestarem serviço de armazenamento e transmissão privada de dados informáticos, exige-se dessas empresas o estrito sigilo ao conteúdo dos e-mails, impõe-se a inviolabilidade dessas informações, tendo como fundamento basilar, inclusive, a proteção constitucional conferida às correspondências (art. 5.º, XII, da CF/1988).[201]

Sendo assim, exsurge a possibilidade de responsabilização desses provedores pelos problemas derivados da prestação do serviço, porém, de mesmo modo, afasta-se a hipótese de penalização por conta de conteúdo postado por terceiro, visto inexistir qualquer "controle editorial" das comunicações trocadas por meio dessas correspondências eletrônicas.[202]

Tal possibilidade restou conjecturada apenas para outras espécies de provedores. Conforme supracitado, o Marco Civil instituiu previsão de responsabilização por danos derivados do conteúdo gerado por terceiro de modo restrito aos provedores de "aplicações de Internet", nomenclatura que, segundo a doutrina, abrangeria os agentes privados relacionados à produção, divulgação ou indicação de acesso ao conteúdo e à sua hospedagem nos meios digitais.

---

[199] Tais como advertência, multa, suspensão temporária das atividades ou proibição do exercício das atividades, a serem aplicadas alternativamente ou cumulativamente, como expõe o art. 12 do Marco Civil. COSTA, Thabata Filizola. **Como era e como é a responsabilidade civil dos provedores de Internet no Brasil?** Mudanças trazidas pelo marco civil da Internet. Disponível em: https://thabatafc.jusbrasil.com.br/artigos/316058731/como-era-e-como-e-a-responsabilidade-civil-dos-provedores-de-internet-no-brasil.

[200] De acordo com referido dispositivo: § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência. BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[201] COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da internet. Revista dos Tribunais, vol. 957, julho de 2015, p. 08. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

[202] Idem.

Essa restrição, em tese, seria justificada em razão do maior grau de contato que tais provedores teriam com os usuários finais, facilitando a fiscalização de suas atividades na rede, além da consequente retirada dos conteúdos ilícitos por eles produzidos. [203]

Por tais razões, o Marco Civil enuncia, em seu artigo 19:

> Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.[204]

Como é possível depreender do referido dispositivo, condicionou-se a responsabilização dos provedores de aplicações à hipótese de descumprimento de ordem judicial expressa, no sentido de contrariar a decisão da Justiça pela retirada de conteúdo ilícito presente em sua plataforma.[205]

Vale destacar que existe um grau de liberdade anterior por parte do agente privado. Antes da manifestação por parte do Judiciário, os provedores possuem poder de escolha quanto à manutenção ou exclusão de determinado material produzido por terceiros em suas páginas, sem estarem sujeitos a penalidades – ao menos a priori.[206]

Apesar disso, o mandamento judicial se sobrepõe a essa esfera de "discricionariedade" do agente privado,[207] visto que, caso o conteúdo seja declarado ilícito, ele haverá necessariamente de ser removido do ciberespaço, sob pena de responsabilização cível subjetiva do provedor.

---

[203] COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da internet. Revista dos Tribunais, vol. 957, julho de 2015, p. 04. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

[204] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[205] REVISTA CONSULTOR JURÍDICO. **STJ divulga precedentes sobre responsabilidade de provedor na internet**. 2017. Disponível em: https://www.conjur.com.br/2017-set-19/stj-reune-precedentes-dever-provedores-internet.

[206] SOUZA, Carlos Affonso; TEFFÉ, Chiara Spadaccini. **Responsabilidade dos provedores por conteúdos de terceiros na internet**. Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet.

[207] ANDRIGHI, Fátima Nancy. **A responsabilidade civil dos provedores de pesquisa via Internet**. Rev. TST. vol. 78, n. 3, jul./set., São Paulo, 2012, p. 72. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=3.

Verifica-se, portanto, que o Marco Civil não impõe a necessidade de uma ordem judicial para a exclusão de todo e qualquer conteúdo da rede, pelo contrário, é facultado ao próprio agente privado a realização da primeira análise acerca da pertinência do material continuar a ser exibido em seu sítio eletrônico.

Evidente que tal autonomia também não pode incorrer em abusos por parte dos entes privados, exige-se, assim, que a filtragem prévia seja fundamentada sob argumentos plausíveis, de modo a evitar possíveis afrontas à liberdade de expressão no âmbito informático – valor expressamente defendido pela Lei n. 12.965/14.[208]

De todo modo, salienta-se a coexistência de dois níveis de verificação da legalidade dos conteúdos digitais: um privado, realizado pelo próprio provedor, sem maiores implicações jurídicas; e outro, público, deliberado pela Justiça, com vistas à definitividade.[209]

Conforme exposto, as notificações extrajudiciais formuladas pelos próprios usuários não dispõem da mesma obrigatoriedade frente ao mandamento expedido pelo Judiciário - em regra, elas se submetem ao arbítrio do provedor, o qual pode decidir por acatar ou não tais solicitações.

No entanto, o Marco Civil impôs algumas excepcionalidades à lógica acima exposta, visto que, para alguns conteúdos de natureza ilícita, o mero requerimento da vítima ou de seu representante legal já possui o condão da obrigatoriedade, gerando responsabilizações ao provedor antes mesmo de qualquer manifestação judicial.

Nesse sentido, como principal exemplo é possível destacar o caput do artigo 21, Lei 12.965/14, cuja redação ressalta o combate às práticas criminosas, tais quais as de “revenge porn”[210]:

---

[208] A liberdade de expressão atua como um norte a todo o Marco Civil, sua garantia está positivada em diversos pontos do diploma, apresenta-se tanto como fundamento (art. 2º) quanto como princípio basilar (art. 3º). BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[209] REVISTA CONSULTOR JURÍDICO. **STJ divulga precedentes sobre responsabilidade de provedor na internet**. 2017. Disponível em: https://www.conjur.com.br/2017-set-19/stj-reune-precedentes-dever-provedores-internet.

[210] COSTA, Thabata Filizola. **Como era e como é a responsabilidade civil dos provedores de Internet no Brasil?** Mudanças trazidas pelo marco civil da Internet. Disponível em: https://thabatafc.jusbrasil.com.br/artigos/316058731/como-era-e-como-e-a-responsabilidade-civil-dos-provedores-de-internet-no-brasil.

> O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.[211]

Assim, verifica-se que, por mais que o Judiciário tenha a legitimidade para chancelar a configuração das ilicitudes praticadas no âmbito digital,[212] a gravidade de alguns crimes fez surgir no Marco Civil uma previsão excepcional, possibilitando que a retirada do conteúdo seja feita de maneira mais ágil, derivada tão somente de uma notificação extrajudicial.[213]

Seja como for, impõe-se a necessidade de uma identificação clara e específica do conteúdo a ser retirado da Internet, de modo a possibilitar a localização inequívoca do material lesivo. Tal determinação[214] se justifica não apenas pela maior eficiência no cumprimento da notificação ou ordem judicial, mas de igual forma, visa-se proteger a liberdade de expressão contra ataques infundados e desnecessários.[215]

No entanto, ainda que o ordenamento jurídico pátrio tenha se atentado à importância que os provedores têm na tratativa dos crimes cibernéticos, verifica-se que tais regulações ainda são insuficientes para a adequada regulamentação da matéria.[216]

---

[211] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[212] ANDRIGHI, Fátima Nancy. **A responsabilidade civil dos provedores de pesquisa via Internet**. Rev. TST. vol. 78, n. 3, jul./set., São Paulo, 2012, p. 72. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=3.

[213] SOUZA, Carlos Affonso; TEFFÉ, Chiara Spadaccini. **Responsabilidade dos provedores por conteúdos de terceiros na internet**. Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet.

[214] A título de exemplo, o parágrafo 1º do artigo 19, Lei 12. 965/14, determina que a ausência dessas informações resulta em nulidade da ordem judicial de retirada do conteúdo ilícito. BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[215] REVISTA CONSULTOR JURÍDICO. **STJ divulga precedentes sobre responsabilidade de provedor na internet**. 2017. Disponível em: https://www.conjur.com.br/2017-set-19/stj-reune-precedentes-dever-provedores-internet.

[216] BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017, p. 90. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.

O Marco Civil inovou em instituir de maneira mais concreta deveres de cooperação e participação desses agentes privados para com as autoridades responsáveis, sejam estas policiais ou judiciárias. Entretanto, percebe-se que as sanções derivadas do descumprimento de tais deveres são, em grande medida, de pouca monta e dificultosa aplicação prática.[217]

Essas complicações se fazem presentes quando da tentativa de responsabilização de um provedor internacional de grande porte. Por mais que a Lei n. 12.965/14 imponha a necessidade de observação da legislação brasileira nos procedimentos de coleta, armazenamento e tratamento dos registros informáticos – com evidente respeito às garantias de privacidade e inviolabilidade dos dados digitais[218] - agentes privados internacionais, por vezes, tem se evadido de seguir à risca tais determinações.[219]

Assim, por mais que se preveja a responsabilização dos provedores, inclusive, pelos danos decorridos de conteúdo de terceiro, questiona-se acerca da aplicabilidade de tal formulação,[220] visto se tratar de uma hipótese excepcional e restrita, relacionada aos agentes de aplicações de Internet, afastando essa penalização de outras espécies de empresas vinculadas ao mercado digital.[221]

Da mesma forma, por mais que a Lei n. 12.965/14 estabeleça outras sanções aos provedores – tais como advertências, suspensão de atividades e até proibição do exercício de suas funções – em casos de descumprimento de deveres de cooperação ou de afronta a ciberdireitos, a doutrina aponta a

---

[217] Nesse sentido, basta memorar dos recorrentes atritos gerados entre a Justiça e o aplicativo de mensagens WhatsApp. Vide a reportagem “Imprensa internacional repercute bloqueio do WhatsApp e cita Cunha”, vinculada no Jornal Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/mercado/2015/12/1720171-midia-internacional-repercute-decisao-de-bloquear-whatsapp-e-cita-cunha.shtml.

[218] BRASIL. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017, p. 76. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.

[219] Ibidem, p. 91.

[220] GALÁN MUÑOZ, Alfonso. **A responsabilidade penal dos provedores de serviço na Internet pela divulgação de conteúdos ilícitos**: uma reflexão inicial sobre o regime espanhol e brasileiro. Revista Justiça e Sistema Criminal, v. 6, n. 11, jul./dez. 2014, p. 96. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30.

[221] Vide o disposto no artigo 18 da Lei n. 12.965/14: “O provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros”. BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

subsistência de lacunas, tal como a falta de delimitação específica de qual a autoridade competente para a condução desse processo.[222]

Nesse sentido, verifica-se que o Marco Civil foi responsável pela implementação, no ordenamento jurídico brasileiro, de relevantes disposições a respeito dos crimes cibernéticos, inclusive quanto ao papel que os agentes privados desempenham nessa tarefa. Contudo, os autores destacam a permanência de alguns impasses, em especial na aplicação prática desses dispositivos legais.

Desse modo, com vistas a permitir uma análise de tais questões sob uma nova ótica, o presente trabalho se propõe a tecer considerações acerca do modelo adotado na Espanha para a responsabilização dos provedores de Internet. Ressaltando-se que, por mais que se reconheçam as particularidades inerentes a cada um dos sistemas jurídicos, é possível compreender como válida a busca por soluções alternativas, verificando possíveis melhorias a serem implementadas na regulamentação brasileira a respeito do tema.

3.3 CONSIDERAÇÕES SOBRE A RESPONSABILIZAÇÃO DOS PROVEDORES PREVISTA NO SISTEMA ESPANHOL

O advento da Sociedade da Informação introduziu grande parte do mundo a um contexto de intensas trocas informacionais. Entretanto, essa mesma sociedade se viu diante de diversos riscos, muitos deles até então inimagináveis, tais como os crimes cibernéticos.

Desse modo, em razão da vasta extensão e capilaridade que caracteriza a Internet nos dias atuais, houve uma proliferação não apenas dos benefícios, mas também dos malefícios inerentes às transformações tecnológicas. Por tais motivos, fez-se necessária a adoção de mecanismos capazes de, ao menos, minimizar essas adversidades.

Assim sendo, tal panorama conduziu a uma multiplicação de normativas estatais e supranacionais acerca da temática, introduzindo a complexidade da Internet no âmbito jurídico, num diálogo entre a proteção dos bens jurídicos

[222] FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital e a sociedade da informação**. – 2. ed. – São Paulo : Saraiva, 2016, p. 255.

relacionados ao desenvolvimento das novas tecnologias e a salvaguarda de valores fundamentais, tais como a liberdade de expressão e de informação.[223]

Nesse sentido, diversos blocos econômicos passaram, no plano regional, a estabelecer marcos legislativos próprios acerca da utilização da Internet, dispondo, inclusive, quanto às possibilidades de responsabilização dos agentes que se valessem da Rede para a prática de ilícitos. No âmbito da União Europeia, por exemplo, aprovou-se a Diretiva 2000/31/CE,[224] a qual dispõe sobre a regulamentação de "serviços da Sociedade de Informação" – sobretudo a respeito do comércio eletrônico desenvolvido no mercado europeu.

A diretiva em questão teve de ser, posteriormente, incorporada aos ordenamentos jurídicos de seus países membros. Na Espanha, por exemplo, isto se deu mediante a aprovação da Lei n. 34/2002,[225] também conhecida como Lei de Serviços da Sociedade da Informação e do Comércio Eletrônico (LSSI), a qual, dentre outras disposições, estabelece o regime de responsabilidade jurídica dos provedores de serviços da Internet.[226]

O referido diploma caracterizou-se por estabelecer regimes de responsabilização diferenciados, específicos para as variadas espécies de prestadores de serviços em atividade no mercado.[227] Sem, contudo, afastar a incidência subsidiária dos ditames gerais de responsabilidade civil, penal e administrativa, previstos por todo o Direito Espanhol.[228]

Contudo, como destaca Galán Muñoz, a LSSI não deve ser entendida como uma lei criada com o intuito de gerar novas formas de penalidades aos

---

[223] GALÁN MUÑOZ, Alfonso. **A responsabilidade penal dos provedores de serviço na Internet pela divulgação de conteúdos ilícitos**: uma reflexão inicial sobre o regime espanhol e brasileiro. Revista Justiça e Sistema Criminal, v. 6, n. 11, jul./dez. 2014, p. 76. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30.

[224] PARLAMENTO EUROPEU. **Diretiva 2000/31/CE**, de 8 de junho de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000L0031.

[225] ESPANHA. **Lei n. 34**, de 11 de julho de 2002. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

[226] GALÁN MUÑOZ, Afonso. **Libertad de expresión y responsabilidad penal por contenidos ajenos en internet**: un estudio sobre la incidencia penal de la ley 34/2002 de Servicios de la Sociedad de la Información y el comercio electrónico. Valencia: Tirant lo Blanch, 2010, p. 63.

[227] PEGUERA POCH, Miquel. **La exención de responsabilidad civil por contenidos ajenos en Internet**. UOC, 2003. Disponível em: https://www.uoc.edu/in3/dt/20080/index.html.

[228] De acordo com o artigo 13.1, LSSI: "Os prestadores de serviços da sociedade da informação estão sujeitos à responsabilidade civil, penal e administrativa estabelecida com caráter geral no ordenamento jurídico, sem prejuízo do disposto nesta Lei". (tradução nossa). ESPANHA. **Lei n. 34**, de 11 de julho de 2002. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

provedores,[229] mas, de modo diverso, teria sido desenvolvida para impor restrições à incidência dessas disposições de caráter geral, facilitando que os agentes privados possam desempenhar o importante papel que lhes cabe na promoção do exercício das liberdades de expressão e de informação.[230]

Segundo o autor, buscou-se evitar que os provedores, intimidados com a possibilidade de serem penalizados pela publicação ou divulgação de conteúdos alheios, passem a retirar de seus sistemas, sem a devida análise, qualquer informação com mínima aparência de ilicitude:[231]

> Opção que, ainda que muito provavelmente, lhes levaria a impedir a publicação de muitas informações penalmente ilícitas ou nocivas, também lhes levaria, certamente, a impossibilitar a divulgação de muitas outras perfeitamente lícitas e permitidas, transformando-se a rede, assim, num meio de comunicação censurado e amordaçado; um ambiente no qual os cidadãos não poderiam exercer de uma forma plena seus direitos à liberdade de expressão e de informação.[232]

Nesse sentido, destacam-se previsões como o artigo 14, LSSI,[233] o qual define que os provedores de transmissão e acesso não serão responsabilizados pela informação transmitida em seus sistemas, salvo nos casos em que eles próprios tenham dado origem à transmissão, modificado os dados ou selecionado os destinatários a serem afetados.[234]

De modo semelhante, é possível também citar seu artigo 16,[235] que estabelece que os provedores de armazenamento não serão responsabilizados

---

[229] GALÁN MUÑOZ, Alfonso. **A responsabilidade penal dos provedores de serviço na Internet pela divulgação de conteúdos ilícitos**: uma reflexão inicial sobre o regime espanhol e brasileiro. Revista Justiça e Sistema Criminal, v. 6, n. 11, jul./dez. 2014, p. 89. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30.

[230] Ibidem, p. 94.

[231] Ibidem, p. 90.

[232] Idem.

[233] Conforme explicita o artigo 14.1, LSSI: "Os operadores de redes de telecomunicações e provedores de acesso a uma rede de telecomunicações que prestem um serviço de intermediação que consista em transmitir por uma rede de telecomunicações dados facilitados pelo destinatário do serviço ou em facilitar acesso a esta não serão responsáveis pela informação transmitida, salvo se eles mesmos tenham originado a transmissão, modificado os dados ou selecionados estes ou aos destinatários dos referidos dados". (tradução nossa). ESPANHA. **Lei n. 34**, de 11 de julho de 2002. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

[234] PEGUERA POCH, Miquel. **La exención de responsabilidad civil por contenidos ajenos en Internet**. UOC, 2003. Disponível em: https://www.uoc.edu/in3/dt/20080/index.html.

[235] O artigo 16.1 explica que: "Os prestadores de um serviço de intermediação consistente em hospedar dados fornecidos pelo destinatário deste serviço não serão responsáveis pela informação armazenada a pedido do destinatário, sempre que: a) Não tenham conhecimento

pelos conteúdos alheios presentes em seus servidores, desde que não possuam efetivo conhecimento da ilicitude ou da capacidade lesiva destes. Na hipótese de os agentes privados terem ciência, a responsabilidade ainda pode ser afastada caso eles procedam com diligência para retirar ou bloquear o acesso a tais materiais.[236]

Verifica-se, portanto, que, mesmo que o provedor obtenha conhecimento acerca da natureza imprópria do conteúdo, sua responsabilização não necessariamente será aplicada, haja vista a possibilidade de isenção pela presteza na cooperação com as autoridades.

Cabe destacar que, ao contrário do modelo adotado pelo Brasil, no Marco Civil da Internet, tal dispensa não decorre da efetiva retirada ou bloqueio do material ilícito, mas sim da forma zelosa pela qual a obrigação é cumprida pelo provedor.[237] De acordo com Galán Muñoz:

> Noutras palavras, o que faz o art. 16.1 "b" LSSI não é criar um novo dever de atuar do provedor que o obriga a apagar ou bloquear o conteúdo em questão e que no caso de ser descumprido torne-o responsável pela divulgação (o dever de garante), mas definir o modo pelo qual haveria de cumprir com dito dever ("com diligência"), quando o tenha, para poder continuar isento de responsabilidade pela prestação de seus serviços.[238]

Tal disposição produz efeitos práticos interessantes, visto que se passa a exigir dos agentes privados um cuidado maior no implemento da ordem judicial de retirada. Não basta apenas eliminar ou bloquear o acesso ao conteúdo de terceiro, impõe-se, na realidade, a busca pelo melhor momento e forma de se realizar tais ações.

Desse modo, compreende-se que a responsabilização pode decorrer pela desídia ou mora do provedor, mas, igualmente, pelo cumprimento apressado ou inadequado da ordem judicial. O referido dispositivo, portanto, valoriza a diligência frente à imediatez, objetivando que a retirada do material

---

efetivo de que a atividade ou a informação armazenada é ilícita ou que lesiona bens ou direito de um terceiro suscetíveis de indenização, ou b) Se o tiver, atuem com diligência para retirar os dados ou tornar impossível o acesso a eles". (tradução nossa). ESPANHA. **Lei n. 34**, de 11 de julho de 2002. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

[236] GALÁN MUÑOZ, Afonso. **Libertad de expresión y responsabilidad penal por contenidos ajenos en internet**: un estudio sobre la incidencia penal de la ley 34/2002 de Servicios de la Sociedad de la Información y el comercio electrónico. Valencia: Tirant lo Blanch, 2010, p. 66.

[237] Ibidem, p. 93.

[238] Ibidem, p. 94.

ilícito seja realizada de modo a garantir o respeito aos direitos da vítima e de terceiros, que poderiam ser afetados com a adoção de alguma medida mais drástica por parte do prestador de serviços.[239]

Outro ponto que merece destaque na legislação espanhola é a exceção prevista contra essas regras gerais de isenção de responsabilidade dos provedores. O artigo 16.2, LSSI, [240] enuncia a possibilidade de penalização das empresas nos casos em que tenham atuado com direção, autoridade ou controle sobre os usuários, na produção desses conteúdos ilícitos.[241]

Nesse sentido, verifica-se que os provedores podem vir a serem responsabilizados pelo material produzido por terceiros na hipótese de estarem diretamente vinculados à divulgação desse conteúdo, numa relação prévia ou concorrente com a conduta de tal usuário.[242] Trata-se de uma situação na qual os prestadores de serviços deixam de serem meros intermediários para se tornarem "verdadeiros editores ou diretores da informação ou do meio utilizado pelo usuário para divulgá-la".[243]

Através dessa analise de alguns dispositivos previstos na lei espanhola, é possível verificar, em primeiro lugar, a existência de diversas similitudes deste modelo em relação ao adotado pelo ordenamento jurídico brasileiro. Em ambos, constata-se a intenção do legislador em restringir o âmbito de responsabilização dos provedores, com vistas a garantir maior fruição das liberdades de expressão e informação no âmbito da Internet, minimizando o risco de censuras e proibições aos seus usuários.[244]

Todavia, ainda que haja algumas críticas quanto ao sistema espanhol, é possível destacar a existência de interessantes inovações quando comparado ao disposto no Marco Civil brasileiro. Conforme exposto, ressalta-se a previsão

---

[239] GALÁN MUÑOZ, Afonso. **Libertad de expresión y responsabilidad penal por contenidos ajenos en internet**: un estudio sobre la incidencia penal de la ley 34/2002 de Servicios de la Sociedad de la Información y el comercio electrónico. Valencia: Tirant lo Blanch, 2010, p. 94.
[240] Ibidem, p. 98.
[241] O artigo 16.2, LSSI menciona que: "A extensão da reponsabilidade estabelecida na seção 1 não operará no caso em que o destinatário do serviço atue sob a direção, autoridade ou controle do seu provedor". (tradução nossa). ESPANHA. **Lei n. 34**, de 11 de julho de 2002. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.
[242] GALÁN MUÑOZ, Alfonso. **A responsabilidade penal dos provedores de serviço na Internet pela divulgação de conteúdos ilícitos**: uma reflexão inicial sobre o regime espanhol e brasileiro. Revista Justiça e Sistema Criminal, v. 6, n. 11, jul./dez. 2014, p. 84. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30.
[243] Ibidem, p. 85.
[244] Ibidem, p. 95.

mais detalhada que a LSSI faz em relação às variadas espécies de provedores, de modo a prever disposições específicas para cada uma delas.

De mesmo modo, tal atenção se faz também perceptível na determinação das hipóteses de responsabilização dos provedores, verifica-se por parte do legislador espanhol um reconhecimento das particularidades e capacidades de cada uma dessas espécies, instituindo penalidades mais pertinentes às atividades desempenhadas por tais agentes privados. [245]

Por fim, destaca-se que o sistema brasileiro de penalização dos provedores está estruturado, em grande medida, sob a lógica civilista. Por mais que o artigo 12 da Lei n. 12.965/14 preveja a possibilidade de incidência de sanções criminais e administrativas, tal disposição é discreta, presente em menor medida do que no diploma espanhol.[246]

Assim sendo, é preciso reconhecer os avanços que o Marco Civil trouxe na regulamentação do uso da Internet e no enfrentamento aos cibercrimes. Através dele houve a positivação de uma série de garantias e direitos aos usuários, instituindo-se deveres para a atuação do poder público, bem como para empresas pertencentes ao setor – principalmente os provedores.

Contudo, é notória entre os autores a subsistência de lacunas e imprecisões técnicas na redação final da Lei n. 12.965/14, com destaque para as disposições a respeito da possibilidade de responsabilização desses provedores de Internet. Nesse sentido, por mais que se reconheça a existência de especificidades entre os ordenamentos jurídicos internacionais, demonstra-se pertinente a análise de modelos implementados em outros países – tal como a Espanha – com vistas a buscar alternativas e propostas de melhorias ao modelo brasileiro.

---

[245] GALÁN MUÑOZ, Alfonso. **A responsabilidade penal dos provedores de serviço na Internet pela divulgação de conteúdos ilícitos**: uma reflexão inicial sobre o regime espanhol e brasileiro. Revista Justiça e Sistema Criminal, v. 6, n. 11, jul./dez. 2014, p. 96. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30.

[246] Idem.

CONSIDERAÇÕES FINAIS

Constatou-se que, para o desenvolvimento do tema com vistas, especialmente, à análise do objetivo geral, fez-se necessário o estudo de diversos aspectos relacionados aos crimes cibernéticos, desde aspectos contextuais, relativos à chamada sociedade da informação e do risco, perpassando pela classificação dos cibercrimes, legislações específicas, procedimento de investigação, alcançando, por fim, o sistema de responsabilização dos provedores.

O estudo permitiu a percepção de que, a despeito dos diversos avanços produzidos acerca da defrontação à criminalidade cibernética subsistem, ainda, diversas lacunas no sistema brasileiro quanto à esses crimes, não apenas em termos legislativos, mas também em relação aos aspectos práticos.

Diante das reflexões realizadas ao longo deste trabalho, percebe-se o quão essencial deve ser a conciliação da teoria com a prática. Explica-se. Não basta apenas a formulação de textos legislativos com capacidade técnica aprimorada em relação aos crimes cibernéticos, mas, igualmente, é de suma importância que sua implantação prática seja acompanhada de uma atuação técnica e especializada, por parte das autoridades competentes.

O sistema jurídico brasileiro acerca dos cibercrimes desenvolveu-se consideravelmente. Não obstante, a aspiração pelo aperfeiçoamento precisa ser contínua, haja vista que tal criminalidade se caracteriza pelo constante dinamismo e mutabilidade em sua expansão.

É evidente, desse modo, que a capacitação das autoridades competentes é de suma importância para a adequada prestação jurisdicional. Porém, entende-se que é igualmente imprescindível a busca por soluções alternativas e inventivas, dentre as quais é possível destacar práticas de conscientização da população acerca dos riscos inerentes a tais tecnologias e das medidas de prevenção a tais delitos.

Assim, são louváveis projetos tais como o “Ministério Público pela Educação Digital nas Escolas”, o qual visa concretizar o dever do Estado em prestar educação quanto “[...] ao uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, para a promoção da

cultura e para o desenvolvimento tecnológico",[247] conforme disposto no artigo 26 do Marco Civil da Internet.[248]

Tal como realizado nesse projeto, a difusão do conhecimento deve ocorrer de maneira inclusiva, destinando-se não apenas às novas gerações, mas abarcando também usuários de mais idade, tendo em vista que estes se revelam vulneráveis em relação aos cibercrimes.

Ao longo do desenvolvimento do presente trabalho foi possível verificar que os crimes cibernéticos apresentam particularidades sensíveis frente a outros delitos, razão pela qual carecem de uma legislação específica, capaz de fornecer artifícios adequados ao enfrentamento dessa criminalidade, sem incorrer em abusos ou violações aos princípios basilares do Direito Penal e Processual Penal.

Os últimos anos foram proveitosos ao trato dos cibercrimes, com especial destaque à promulgação de diplomas legais diretamente relacionados à temática. Não obstante, verifica-se que ainda há um longo caminho a ser trilhado no Brasil.

Como visto, a criação de um arcabouço jurídico apropriado deve ser, necessariamente, acompanhado de um aprimoramento na sua aplicabilidade prática. É essencial que haja dispositivos legais mais específicos sobre crimes cibernéticos, porém, estes apenas terão plena eficácia se complementados por atuação especializada e integrada dos agentes públicos – inclusive com agentes privados - de maneira a formar uma verdadeira rede de prevenção e resolução de tais delitos.

---

[247] BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Crimes Cibernéticos** – Brasília: MPF, 2018, p. 257. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.

[248] De acordo com o art. 26 da Lei n. 12.965/14: "O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico". BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRIGHI, Fátima Nancy. **A responsabilidade civil dos provedores de pesquisa via Internet**. Rev. TST. vol. 78, n. 3, jul./set., São Paulo, 2012, p. 65. Disponível em: https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=3.

ARAGÃO, David Farias de. **Crimes Cibernéticos na Pós-Modernidade**: direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil. 2015. Dissertação (Mestrado em Direito) – Universidade Federal do Maranhão, São Luís. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/667

BARRETO, Alessandro Gonçalves; BARRETO, Karolinne Brasil. **Lei 13.718/18**: criminalização da divulgação de cena de sexo, nudez e pornografia sem consentimento da vítima e outros delitos. Disponível em: https://www.migalhas.com.br/dePeso/16,MI288717,81042-Lei+1371818+criminalizacao+da+divulgacao+de+cena+de+sexo+nudez+e.

BECK, Ulrich. **A metamorfose do mundo**: como as alterações climáticas estão a transformar a sociedade. – Lisboa: Edições 70, 2016.

_____. **Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Ed. 34, 2010.

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte geral 1. – 24. ed. – São Paulo: Saraiva Educação, 2018.

BORTOT, Jessica Fagundes. **Crimes Cibernéticos**: aspectos legislativos na persecução penal com base nas legislações brasileira e internacional. Virtuajus (PUCMG), v. 13, p. 298-322, 2017. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745.

BRASIL. **Código Penal**. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

_____. **Código de Processo Penal**. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm.

_____. Superior Tribunal de Justiça. **Conflito de Competência nº 121.431-SE** – Distrito Federal. Relator: Min. Marco Aurélio Bellizze. Disponível em: http://www.mp.go.gov.br/portalweb/hp/7/docs/stj-orkut-conflito-competenci.pdf.

_____. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm.

_____. Supremo Tribunal Federal. **Habeas Corpus nº 76.689 - PB** – 1ª Turma. Distrito Federal. Relator: Min. Sepúlveda Pertence. Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo130.htm.

_____. Tribunal Regional da 3ª Região. Escolas de Magistrados. **Investigação e prova nos crimes cibernéticos**. - São Paulo: EMAG, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf.

_____. **Lei nº 7.716**, de 5 de janeiro de 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716.htm.

_____. **Lei nº 9.100**, de 29 de setembro de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9100.htm.

_____. **Lei nº 9.609**, de 19 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm.

_____. **Lei nº 9.983**, de 14 de julho de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9983.htm.

_____. **Lei nº 11.829**, de 25 de novembro de 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm.

_____. **Lei nº 12.034**, de 29 de setembro de 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12034.htm.

_____. **Lei nº 12.735**, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.

_____. **Lei nº 12.737**, de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm.

_____. **Lei nº 12.965**, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

_____. **Lei 13.718/2018,** de 24 de setembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13718.htm.

_____. **Projeto de Lei nº 84, de 1999**. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=23342A6D4FB1ED35373900C1A5590713.node2?codteor=1034065&filename=Avulso+-PL+84/1999.

_____. **Projeto de Lei nº 2793, de 2011**. Disponível em: https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218.

_____. **Projeto de Lei n. 5452, de 2016**. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A24E46AE366969B7F42D0D5449FF6258.proposicoesWebExterno2?codteor=1630876&filename=Avulso+-PL+5452/2016.

_____. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf.

BRITO, Auriney. **Análise da Lei 12.737/12**: Lei Carolina Dieckmann. Disponível em: http://politicacidadaniaedignidade.blogspot.com/2013/04/analise-da-lei-1273712-lei-carolina.html.

BUSATO, Paulo César. **Direito penal**: parte especial 1. – 2 ed. – São Paulo: Atlas, 2016.

_____. **Direito penal**: parte especial 2, v.3. – São Paulo: Atlas, 2017.

_____. **Direito penal**: parte geral. – 2. ed – São Paulo: Atlas, 2015.

BORTOT, Jessica Fagundes. **Crimes Cibernéticos**: aspectos legislativos na persecução penal com base nas legislações brasileira e internacional. Virtuajus (PUCMG), v. 13, 2017, p. 359. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/view/15745.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. – Rio de Janeiro: Jorge Zahar Ed., 2003.

CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **A Sociedade em Rede**: do conhecimento à ação política; Conferência. Belém (Por): Imprensa Nacional, 2005. Disponível em: http://www.egov.ufsc.br/portal/conteudo/sociedade-em-rede-do-conhecimento-%C3%A0-ac%C3%A7%C3%A3o-pol%C3%ADtica.

COLAÇO, Hian Silva. **Responsabilidade civil dos provedores de Internet**: diálogo entre a jurisprudência e o marco civil da internet. Revista dos Tribunais, vol. 957, julho de 2015, p. 06. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.957.05.PDF.

COSTA, Thabata Filizola. **Como era e como é a responsabilidade civil dos provedores de Internet no Brasil?** Mudanças trazidas pelo marco civil da Internet. Disponível em:

https://thabatafc.jusbrasil.com.br/artigos/316058731/como-era-e-como-e-a-responsabilidade-civil-dos-provedores-de-internet-no-brasil.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. – São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches. **Lei 13.718/18:** Introduz modificações nos crimes contra a dignidade sexual. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2018/09/25/lei-13-71818-introduz-modificacoes-nos-crimes-contra-dignidade-sexual.

ESPANHA. **Lei n. 34**, de 11 de julho de 2002. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital e a sociedade da informação**. – 2. ed. – São Paulo : Saraiva, 2016.

FRANÇA. **Declaração de Direitos do Homem e do Cidadão,** 26 de agosto de 1789. Disponível em: http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem_cidadao.pdf.

GALÁN MUÑOZ, Alfonso. **A responsabilidade penal dos provedores de serviço na Internet pela divulgação de conteúdos ilícitos**: uma reflexão inicial sobre o regime espanhol e brasileiro. Revista Justiça e Sistema Criminal, v. 6, n. 11, jul./dez. 2014, p. 96. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30.

_____. **Libertad de expresión y responsabilidad penal por contenidos ajenos en internet**: un estudio sobre la incidencia penal de la ley 34/2002 de Servicios de la Sociedad de la Información y el comercio electrónico. Valencia: Tirant lo Blanch, 2010.

GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora UNESP, 1991.

GLANZ, Semy. **Internet e Contrato Eletrônico**. Revista da EMERJ, v.1, n.3, 1998.Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/revista03_94.pdf.

HUNGRIA. **Convenção sobre o Cibercrime.** Aberta para assinatura em Budapeste, Hungria, em 22 de novembro de 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. – São Paulo: Saraiva, 2016.

LEMOS, André. **A Comunicação das Coisas. Internet das Coisas e a Teoria Ator-Rede**: Etiquetas de radiofrequência em uniformes escolares na Bahia. Apresentado no SimSocial, 2012. Salvador, Bahia, outubro.Disponível em: http://roitier.pro.br/wp-content/uploads/2017/09/Andre_Lemos.pdf.

LORENZETTI, Jorge; TRINDADE, Letícia de Lima; PIRES, Denise Elvira de Pires; RAMOS, Flávia Regina Souza. **Tecnologia, inovação tecnológica e saúde**: uma reflexão necessária. Texto Contexto Enferm, Florianópolis, 2012 Abr-Jun; 21(2): 432-9, p. 436. Disponível em: http://www.scielo.br/pdf/tce/v21n2/a23v21n2.pdf.

MUÑOZ CONDE, Francisco; GARCÍA ARÁN, Mercedes. **Derecho Penal**: parte general – 8. ed. – Valência: Tirant Lo Blanch, 2010.

OLIVEIRA, Marcel Gomes. **As inovações legislativas aos crimes sexuais no enfrentamento à criminalidade**: comentários à lei n. 13.718/18. Disponível em: http://emporiododireito.com.br/leitura/as-inovacoes-legislativas-aos-crimes-sexuais-no-enfrentamento-a-criminalidade-comentarios-a-lei-n-13-718-2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos,** 10 de dezembro de 1948. Disponível em:https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf.

_____. **Pacto Internacional dos Direitos Civis e Políticos**, 16 de dezembro de 1966. Disponível em: https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Pol%C3%ADticos.pdf

PARLAMENTO EUROPEU. **Diretiva 2000/31/CE**, de 8 de junho de 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000L0031.

PEGUERA POCH, Miquel. **La exención de responsabilidad civil por contenidos ajenos en Internet**. UOC, 2003. Disponível em: https://www.uoc.edu/in3/dt/20080/index.html.

PIAUHYLINO, Luiz. **Projeto de Lei nº 84, de 1999**. Dispõe sore os crimes cometidos na área da informática, suas penalidades e dá outras providências. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=23342A6D4FB1ED35373900C1A5590713.node2?codteor=1034065&filename=Avulso+-PL+84/1999.

REVISTA CONSULTOR JURÍDICO. **STJ divulga precedentes sobre responsabilidade de provedor na internet**. 2017. Disponível em: https://www.conjur.com.br/2017-set-19/stj-reune-precedentes-dever-provedores-internet.

ROSA, Giovanni Santa. **Na era do wi-fi, a internet ainda depende de cabos para existir**. Disponível em: https://tecnologia.uol.com.br/noticias/redacao/2018/03/18/na-era-do-wi-fi-a-internet-ainda-depende-de-cabos-para-existir.htm.

SANTOS, Vinicius Wagner Oliveira. **Neutralidade da rede e o Marco Civil da Internet no Brasil**: atores, políticas e controvérsias. 2016. Tese (Doutorado em Direito) - Universidade Estadual de Campinas, Campinas, p. 148-149. Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/321453/1/Santos_ViniciusWagnerOliveira_D.pdf.

SEGER, Alexander. **Cybercrime Training for Judges**: training manual. – Strasbourg: Economic Crime Division, Council of Europe, 2010. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/dados-da-atuacao/eventos-2/eventos-internacionais/conteudo-banners-1/crimes-ciberneticos/cybercrime-training-for-judges-training-manual/view.

_____. **The Budapest Convention on Cybercrime 10 years on**: lessons learnt or the web is a web. Mont Blanc, p.1-7, 2012. Disponível em: https://rm.coe.int/16802fa3e0.

SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**: perspectivas e limites. Tese de doutorado. Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2137/tde-30112015-165420/pt-br.php.

SOUZA, Carlos Affonso; TEFFÉ, Chiara Spadaccini. **Responsabilidade dos provedores por conteúdos de terceiros na internet**. Disponível em: https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-internet.

SOUZA, João Éder Furlan Ferreira de. **Desigualdade digital no Brasil:** Desafios jurídico-políticos para uma sociedade informacional inclusiva. Dissertação de mestrado. Programa de Pós-Graduação em Ciência Jurídica, Universidade Estadual do Norte do Paraná, Jacarezinho, 2017. Disponível em: https://uenp.edu.br/pos-direito-teses-dissertacoes-defendidas/direito-dissertacoes/9681-joao-eder-furlan-ferreira-de-souza/file.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. – 2. ed. – São Paulo: Saraiva, 2015.

TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil**: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/livroverde.pdf.

TEIXEIRA, Paulo; Erundina, Luiza; D'ávila, Manuela; Arruda, João; Neto, Brizola; José, Emiliano. **Projeto de Lei nº 2793, de 2011**. Dispõe sobre a

tipificação criminal de delitos informáticos e dá outras providências. Disponível em: https://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218.

TRUZZI, Gisele; DAOUN, Alexandre. **Crimes informáticos**: o direito penal na era da informação. In: *Proceedings of the Second Internacional Conference of Forensic Computer Science*, Guarujá (SP), ABEAT, p. 115-120, 2007. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf

VERDELHO, Pedro. **The Effectiveness of International Co-operation against Cybercrime:** examples of good practice. Strasbourg, p. 4-37, 2008. Disponível em: https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/DOC-567study4-Version7_en.PDF

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**: conforme a Lei nº 12.737/2012. – Belo Horizonte: Editora Fórum, 2013.

WANG, Qianyun. **A Comparative Study of Cybercrime in Criminal Law**: China, US, England, Singapore and the Council of Europe. Tese de doutorado. Erasmus University Rotterdam, Roterdã, 2016, p. 05. Disponível em: https://www.bibliotheek.nl/catalogus/titel.408161779.html/a-comparative-study-of-cybercrime-in-criminal-law--china--us--england/.

WENDT, Emerson. **Inteligência cibernética**: da ciberguerra ao cibercrime a (in)segurança virtual no Brasil, - São Paulo: Editora Delfos, 2011.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013.

WERLE, Vera Maria; OLIVEIRA, Bruna Machado de; MATTOS, Karoline Reis; SIQUEIRA, Marcela Scheuer. **Crimes virtuais e a legislação brasileira**. (Re) Pensando Direito, EDIESA, Ano 7, n. 13, jan./jun., 2017, p. 128-129. Disponível em: http://local.cnecsan.edu.br/revista/index.php/direito/article/viewFile/468/342.