UNIVERSIDADE FEDERAL DE UBERLÂNDIA – UFU
FACULDADE DE DIREITO "PROF. JACY DE ASSIS" – FADIR GRADUAÇÃO EM DIREITO

VINICIUS MILANI DEL PUPO

ATIVIDADE PROBATÓRIA NOS CIBERCRIMES

UBERLÂNDIA/MG
2022

VINICIUS MILANI DEL PUPO

ATIVIDADE PROBATÓRIA NOS CIBERCRIMES

Trabalho de Conclusão de Curso ou Dissertação ou Tese apresentado à Faculdade de Direito da Universidade Federal de Uberlândia como requisito básico para a conclusão do Curso de Direito.

Orientador: Professor Mestre Karlos Alves Barbosa

UBERLÂNDIA/MG
2022

ATIVIDADE PROBATÓRIA NOS CIBERCRIMES

Trabalho de conclusão de curso orientado pela Professor Mestre Karlos Alves Barbosa, apresentado à Faculdade de Direito da Universidade Federal de Uberlândia-UFU, como requisito para obtenção do grau de bacharel em Direito, aprovado pela banca examinadora formada por:

Uberlândia, _ de _____ de 2023.

_____

Professor Mestre Karlos Alves Barbosa

Orientador – Professor Mestre da UFU

_____

Professor Doutor Edihermes Marques Coelho

Professor Doutor da UFU

_____

Professora Simone Silva Prudêncio

Professora Doutora da UFU

UBERLÂNDIA/MG

2022

RESUMO

A popularização da *internet* e o desenvolvimento tecnológico possibilitaram a ocorrência de uma nova modalidade de crimes: os cibercrimes. Com isso, o legislador brasileiro visando cobrir as lacunas no ordenamento jurídico geradas com essa nova atividade, criou legislações de modo a tipificá-las, entretanto ignorou as características peculiares desse novo ilícito, principalmente ao que se refere a atividade probatória e a necessidade de cooperação internacional, o que resultou em um cenário de impunidade e rápida expansão da atividade criminosa, contexto que permanece até os dias atuais e levou a recente adesão do Brasil à Convenção de Budapeste. Assim, o presente artigo tem por finalidade fazer uma análise da atividade probatória nos cibercrimes, observando as características próprias das provas digitais e realizando um paralelo entre a evolução histórica brasileira e mundial, com o intuito de captar as problemáticas e apresentar sugestões e experiências de outros países também signatários à convenção, de modo a fornecer elementos para que o legislador, considerando as peculiaridades próprias de nosso país, escolha a melhor estratégia de combate aos crimes praticados na *internet*.

Palavras-Chave: Crimes virtuais. Cibercrimes. *Internet*. Rede mundial de computadores. Convenção de Budapeste. Convenção sobre o Cibercrime. Prova digital.

ABSTRACT

The popularization of the internet and the technological development have enabled the occurrence of a new type of crimes: cybercrimes. With this, the Brazilian legislature, aiming to cover the gaps in the legal system generated by this new activity, created laws in order to typify them, however, ignored the peculiar characteristics of this new offense, especially with regard to the evidential activity and the need for international cooperation, which resulted in a scenario of impunity and rapid expansion of criminal activity, a context that remains until today and led to the recent accession of Brazil to the Budapest Convention. Thus, this article aims to analyze the evidential activity in cybercrimes, observing the characteristics of digital evidence and making a parallel between the Brazilian and world historical evolution, in order to capture the problems and present suggestions and experiences of other countries that are also signatories to the convention, so as to provide elements for the legislator, considering the peculiarities of our country, to choose the best strategy to combat crimes committed on the Internet.

Keywords: Cybercrime. Cybercrimes. Internet. World Wide Web. Budapest Convention. Convention on Cybercrime. Digital evidence.

SUMÁRIO

1. INTRODUÇÃO

A revolução tecnológica, iniciada no século XX e ainda em curso, promoveu profundas transformações na sociedade e em seu modo de se relacionar, principalmente, com o advento da *internet*, rede mundial de computadores capaz de interligar computadores do mundo inteiro, proporcionando uma maior facilidade de comunicação.

O impacto dessa revolução tecnológica resultou na formação da chamada sociedade da informação, caracterizada pela importância cada vez maior da informação e pela dependência também cada vez maior dos recursos tecnológicos em atividades cotidianas.

Embora essa nova realidade tenha gerado diversos benefícios para a sociedade, há de se ressaltar que ela propiciou o aparecimento de um novo tipo de criminalidade: a cibercriminalidade.

A aplicabilidade do direito à Sociedade de Informação sempre levantou alguns problemas devido à dificuldade da legislação processual penal para se adaptar com a mesma velocidade das novas invenções, além do fato de os métodos tradicionais de direito se demonstraram obsoletos frente a constante evolução dos infratores, principalmente no que se refere a atividade probatória.

Na contramão das exigências, o legislador brasileiro não observou a complexidade que envolve os crimes praticados na *internet* e optou por combater a cibercriminalidade através de meios tradicionais de investigação e simples legislações especificas que apenas tipificavam os delitos sem quaisquer previsões processuais, o que se demonstrou ineficaz, gerando um cenário de impunidade e rápida expansão da atividade criminosa.

Diante desse caos, o legislador reconheceu a necessidade de um aparato legislativo processual específico e um sistema de cooperação internacional. Assim, em dezembro de 2021, o Brasil aderiu à Convenção sobre o Cibercrime, comprometendo-se a realizar as alterações legislativas necessária para se adequar à Convenção.

Sendo assim, o presente estudo tem por objetivo apresentar - após uma breve análise histórica sobre o tratamento disposto aos cibercrimes no Brasil e em alguns países signatários da convenção – diferentes soluções relacionadas a atividade probatória encontradas por outros países para se adaptar à Convenção sobre o Cibercrime, de modo a contribuir com que as

autoridades escolham a melhor opção de acordo com nossas características próprias, garantindo um resultado satisfatório no combate à impunidade das infrações cometidas no ciberespaço.

2. PROVAS

2.1 CONCEITO E FINALIDADE DA PROVA

De acordo com Nucci, o termo prova origina-se do latim *probatio*, que por sua vez deriva o verbo provar – *probare* -, significando ensaiar, verificar, examinar, reconhecer por experiência, aprovar, estar satisfeito com algo, persuadir alguém a alguma coisa ou demonstrar.[1]

A doutrina divide o termo prova em três sentidos, de acordo com Nucci, são elas:

> a) como ato: é o processo pelo qual se verifica a exatidão do fato alegado pela parte (ex.: fase da prova); b) como meio: trata-se do instrumento pelo qual se demonstra a verdade de algo (ex.: prova testemunhal); c) como resultado: é o produto extraído da análise dos instrumentos de prova oferecidos, demonstrando a verdade de um fato.[2]

Corrobora com esse entendimento Aury Lopes Jr., o qual afirma que através – essencialmente - das provas, o processo penal pretende criar condições para que o juiz exerça sua atividade recognitiva, a partir da qual se produzirá o convencimento externado na sentença. De modo que, é a prova que permite a atividade recognoscitiva do juiz em relação ao fato histórico (*story of the case*) narrado na peça acusatória.[3]

Durante a fase de instrução, é feita à apuração de determinados fatos, a fim de convencer o juiz que o acusado deverá ser condenado. "Essa demonstração a respeito da veracidade ou falsidade da imputação, que deve gerar no juiz a convicção de que necessita para o seu pronunciamento é o que constitui a prova"[4].

---

[1] NUCCI, Guilherme de Souza. **Provas no Processo Penal**. 4 ed. Rio de Janeiro: Forense, 2015, p. 21.
[2] Ibidem, p. 24.
[3] LOPES JR., Aury. **Direito processual Penal**. 14 ed. São Paulo: Saraiva, 2017, p. 342.
[4] MIRABETE, Julio Fabbrini. **Código de Processo Penal Interpretado**. 11 ed. São Paulo: Atlas, 2007, p. 453.

Portanto, a prova é fundamental para o convencimento do magistrado, sendo por meio da apreciação das provas nos autos que o julgador decide pela condenação ou absolvição do réu.

2.2 SISTEMAS DE APRECIAÇÃO DE PROVAS

O sistema de provas, na definição de Paulo Rangel, é o critério utilizado pelo juiz para valorar as provas dos autos, alcançando a verdade histórica do processo.[5]

São três os principais sistemas probatórios catalogados, quais sejam, o sistema legal de provas, também conhecido como sistema da prova tarifada; o sistema da intima convicção, também conhecido como sistema da certeza moral; e, por último, o sistema do livre convencimento motivado, também conhecido como sistema da persuasão racional.

Segundo Nestor Távora, as regras de apreciação adotadas demonstram a transparência no ato de julgar, uma vez que revelam o porquê do convencimento do juiz, qual o direcionamento do magistrado quando da tomada de sua decisão.[6]

No sistema da íntima convicção, destaca-se a liberdade do juiz para decidir sem qualquer obrigação de motivar a sua decisão. Nesse sistema não há qualquer regra de valoração das provas, podendo o magistrado inclusive se utilizar de suas crenças pessoais para tomar a sua decisão.

Discorrendo acerca do sistema da íntima convicção Julio Fabbrini Mirabete leciona que:

> Pelo sistema da certeza moral do juiz, ou da íntima convicção, a lei nada diz sobre o valor das provas e a decisão funda-se exclusivamente na certeza moral do juiz, que decide sobre sua admissibilidade, sua avaliação, seu carreamento para os autos. É o sistema que preside, de certo modo, os julgamentos efetuados pelo tribunal de Júri.[7]

---

[5] RANGEL, Paulo. **Direito Processual Penal**. 23 d. São Paulo. Atlas. 2015, p. 515.
[6] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. Salvador: Jus Podivm, 2012, p. 398.
[7] MIRABETE, Julio Fabrini. **Processo Penal**. 18 ed. São Paulo: Atlas, 2006, p. 260.

Enquanto no sistema da certeza moral do legislador, a lei estabelece o valor de cada meio de prova com o fim de que o magistrado o considere como base para a formação de sua decisão, retirando qualquer liberdade do julgador de apreciação da prova.

Sobre o sistema da certeza moral do legislador, adverte Fernando Capez que:

> A lei impõe ao juiz o rigoroso acatamento a regras preestabelecidas, as quais atribuem, de antemão, o valor de cada prova, não deixando para o julgador qualquer margem de discricionariedade para emprestar-lhe maior ou menor importância. Não existe convicção pessoal do magistrado na valoração do contexto probatório, mas obediência estrita ao sistema de pesos e valores imposto pela lei. [8]

Por fim, o sistema da persuasão racional pela qual o legislador tem liberdade para decidir e apreciar as provas, não havendo limitação a qualquer critério legal de fixação de valores probatórios, desde que o faça de maneira motivada, nos termos do art. 155 do Código de Processo Penal, portanto este é o sistema adotado pela legislação brasileira atual.

Sobre o sistema da persuasão racional acrescenta Fernando Capez advertindo que:

> O juiz tem liberdade para formar a sua convicção, não estando preso a qualquer critério legal de prefixação de valores probatórios. No entanto, essa liberdade não é absoluta, sendo necessária a devida fundamentação. O juiz, portanto, decide livremente de acordo com a sua consciência, devendo, contudo, explicitar motivadamente as razões de sua opção e obedecer a certos balizamentos legais, ainda que flexíveis. [9]

O sistema da persuasão racional representa um equilíbrio entre os demais sistemas, pois assim como não existe uma liberdade absoluta quando o juiz tem que decidir a respeito do litígio, necessitando fundamentar a sua decisão motivadamente, e, em contrapartida não existe uma liberdade absoluta quando se trata dos meios de provas permitidos na busca da comprovação dos fatos alegados no processo.

---

[8] CAPEZ, Fernando. **Curso de Processo Penal**. 12 ed. São Paulo: Saraiva, 2005, p. 275.
[9] CAPEZ, 2005, p. 276.

2.3 MEIOS DE PROVA

Os meios de prova são as vias pelas quais as partes podem se utilizar, direta ou indiretamente, para comprovar a veracidade dos fatos alegados, ou seja, é tudo aquilo que pode ser utilizado para apuração da verdade real.

Neste sentido ensina Júlio Fabbrini Mirabete que:

> Meios de prova são as coisas ou ações utilizadas para pesquisar ou demonstrar a verdade: depoimentos, perícias, reconhecimentos etc. Como no processo penal brasileiro vige o princípio da verdade real, não há limitação dos meios de prova. A busca da verdade material ou real, que preside a atividade probatória do juiz, exige que os requisitos da prova no sentido objetivo se reduzem ao mínimo, de modo que as partes possam utilizar-se dos meios de prova com ampla liberdade. Visando o processo penal o interesse público ou social de repressão ao crime, qualquer limitação à prova prejudica a obtenção da verdade real e, portanto, ajusta aplicação da lei. [10]

O Código de Processo Penal Brasileiro traz um rol de meio de provas admissíveis, as quais denominamos de provas nominadas, entretanto não podemos esquecer que no Processo Penal vigora o princípio da verdade real, do qual deriva-se o princípio da liberdade probatória, o que implica na plena utilização de meios probatórios idôneos para formação da convicção do juiz, mesmo que não haja previsão expressa no ordenamento jurídico.

Desse modo o rol presente no Código de Processo Penal é meramente exemplificativo, assim, na busca da verdade dos fatos, é admitido, além das provas nominadas, a utilização das provas inominadas, quais sejam, aquelas provas que não estão elencadas no ordenamento jurídico. Portanto, as limitações aos meios de provas são exceções.

Contudo, a utilização das provas inominadas deve respeitar os limites constitucionais e processuais da prova, sob pena de ilicitude ou ilegitimidade dessa prova.

Sobre o assunto, Fernando Capez adverte que a "prova vedada ou proibida é, portanto, aquela produzida por meios ilícitos, ou seja, em contrariedade a uma norma legal específica. A prova vedada comporta duas espécies distintas: (a) prova ilegítima e (b) prova ilícita." [11]

---

[10] MIRABETE, 2006, p. 252.
[11] CAPEZ, 2005, p. 278.

As provas ilícitas são aquelas que violam regra de direito material ou a Constituição no momento que são coletadas. Desse modo, o vício está no momento de obtenção da prova, ou seja, quando afrontado um direito que determinado indivíduo tem tutelado independentemente do processo. Essas provas necessitam de um cuidado especial, pois caso se tornem ilícitas deverão ser desentranhadas do processo, já que não são passíveis de repetição.

Já à prova ilegítima são aquelas cuja colheita estaria ferindo normas de direito processual. Nesse caso, há violação de norma garantidora de interesse vinculado ao processo e sua finalidade, ou seja, a prova ilegítima viola o devido processo legal, visto do prisma formal e não substancial como a ilícita.

Sobre a diferença, afirma Alexandre de Moraes:

> As provas ilícitas são aquelas obtidas com infringência ao direito material, as provas ilegítimas são as obtidas com desrespeito ao direito processual. Por sua vez, as provas ilegais seriam o gênero do qual as espécies são as provas ilícitas e as ilegítimas, pois configuram-se pela obtenção com violação de natureza material ou processual ao ordenamento jurídico.[12]

A questão dos meios de prova está intimamente relacionada aos crimes cibernéticos, uma vez que os pilares a qual se norteia o processo penal brasileiro não se adaptou em tempo para suprir as novas demandas trazidas pelos delitos surgidos com advento da *internet*, caracterizados pela celeridade e dinamismo, o que gera diversos obstáculos e particularidades na busca pela verdade e na solução de tais crimes.

3. PROVAS DIGITAIS

As provas digitais são os principais tipos de provas utilizadas para elucidação dos crimes cibernéticos. Esse tipo de prova apresenta várias peculiaridades que acabam por transformar a atividade probatória nesse tipo penal em um processo árduo e complexo, de modo que os meios tradicionais utilizados nos crimes em geral se demonstram obsoletos. Sendo assim, seu estudo se apresenta como um importante passo para a compreensão das dificuldades geradas durante a obtenção de provas.

---

[12] MORAES, Alexandre de. **Direito Constitucional**. 27 ed. São Paulo: Atlas, 2011, p. 117.

3.1 CONCEITO

O desenvolvimento tecnológico e científico propiciou o surgimento de um novo delito penal, os chamados crimes cibernéticos, caracterizados, principalmente, pela sua celeridade, dinamismo, capacidade de adaptação e facilidade de ação.

Ocorre que, a legislação processual penal não se adaptou com a mesma velocidade das novas invenções e os métodos tradicionais de direito se demonstraram obsoletos frente a constante evolução dos infratores. Assim, aumentou-se as dificuldades das autoridades judiciárias de aplicar sanções a esses delitos, fazendo com que o ambiente virtual tenha aromas de impunidade.

Utilizando-se da definição de Armando Dias Ramos a prova digital "é a informação passível de ser extraída de um dispositivo eletrônico (local, virtual ou remoto) ou de uma rede de comunicações. Pelo que esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta."[13]

3.2 NECESSIDADE DE PERÍCIAS ESPECIALIZADAS

A aplicação de sanções nos cibercrimes não se trata de algo simples, pois a obtenção das provas digitais é sempre acompanhada de um processo árduo e trabalhoso, que implica em diversas dificuldades.

Diante dessas dificuldades se faz importante a presença de perícias especializadas. Essa necessidade culminou no surgimento da computação forense, cujo objetivo é a investigação e a coleta de evidências das condutas ilícitas praticadas por meio de computadores.[14]

A prova digital consiste em uma prova imaterial, portanto o investigador forense deve ser conhecedor de técnicas específicas para dar uso de palavras-chave ou servir-se de técnicas

---

[13] RAMOS, Armando Dias. **A Prova Digital em Processo Penal.** Lisboa: Chiado Editora, 2014, p. 86.
[14] RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses na investigação digital. **Revista de Engenharia e Tecnologia**, Ponta Grossa, v.2, n. 3, nov. 2010. Disponível em: <http://ri.uepg.br/riuepg/bitstream/handle/123456789/530/ARTIGO_AnaliseFerramentasForenses.pdf?sequence=1>. Acesso em: 29 set. 2022. P. 1.

de desencriptação, vez que à complexidade e codificação constituem características desse tipo de prova, sob risco de se tornarem inutilizáveis nos casos em que o investigador a altere significativamente, por desconhecer a sua presença.[15]

Em alguns casos, a investigação forense precisará lidar com provas fragmentadas, ou seja, as provas poderão se encontrar distribuídas por vários terminais, computadores e redes que se estendem por uma vasta área espacial ou geográfica. [16]

A identificação da localização é outro obstáculo, uma vez que o crime cibernético não tem fronteiras, desse modo a busca da prova digital, não incide desde logo, na identificação do local onde é cometido o crime, pois a realização desse tipo de crime pode se dar de qualquer lugar do mundo, basta que haja um dispositivo conectado à *internet*. Além do mais, em várias situações que se faz necessário a Prova Digital para conclusão de determinado inquérito, sequer a uma ligação entre o infrator e o objeto do crime, sendo este cometido a distância.

Sobre esse assunto expõe Jacqueline Lafloufa:

> O problema do mundo digital, contudo, é que ele não tem fronteiras, enquanto que a legislação é aplicada de acordo com a localidade de realização do suposto crime cibernético. Sabendo disso, hackers de todo o mundo têm aprendido a burlar as leis, hospedando seus sites em países de legislação mais flexível, como a Eslovênia ou a Suíça, e usando artimanhas digitais para que seus acessos via *IP* apontem para regiões onde a punição judicial a cibercrimes seja mais difícil, com o uso de *proxys*, sites da web que permitem a navegação de forma supostamente anônima, ao trocar o *IP* que identifica o computador que realiza determinado acesso.[17]

Sobre a utilização da prova digital, umas das dificuldades provém da sua natureza volátil, instável, frágil e alterável apresentando há possibilidade de alteração ou desaparecimento. Devido à presença apenas no ambiente virtual, este tipo de prova apresenta certa facilidade para que os registros sejam apagados ou alteradas, de forma que não haja

---

[15] CANCELA, Alberto Gil Lima. **A prova digital**: os meios de obtenção de prova na Lei do Cibercrime. 2016. 78 f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de Coimbra, Coimbra, 2016. Disponível em: <https://core.ac.uk/download/pdf/43589323.pdf>. Acesso em: 26 set. 2022. P. 22.

[16] RODRIGUES, Benjamim Silva. **Das Escutas Telefónicas – À Obtenção da Prova (Em Ambiente) Digital**. 2 ed. Coimbra: Coimbra Editora, 2009, p. 726.

[17] LAFLOUFA, Jacqueline. Hackativismo: crime cibernético ou legítima manifestação digital?. **ComCiência,** Campinas, n. 131, 2011. Disponível em: <http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542011000700006&lng=pt&nrm=iso>. Acesso em: 11 de out. 2022.

qualquer indício probatório que o crime foi cometido em determinado local ou em determinado dispositivo, eliminando qualquer vestígio que permita relacionar o crime a ação do agente que o cometeu.

Ademais, provindo da constante mutabilidade que lhe caracteriza, pode haver situações em que o investigador se depara inicialmente com uma prova com certas características, e mais tarde, está se modifica, total ou parcialmente.

Esse fato exige que o investigador forense redobre os cuidados ao recolher as provas, devendo identificar, de forma ainda mais rigorosa, qual o tipo de prova digital em causa. Apenas com essa identificação, poderá o investigador garantir a força probatória da prova digital, sem perigo de esta ser alterada ou desaparecer.[18]

Importante ressaltar que o investigador deve alinhar, a celeridade em que a prova digital exige para ser recolhida com todos os cuidados necessários, sob pena de perder integridade, o que torna a tarefa de alta complexidade.

A atenção ainda deve estar presente para a determinação do momento, pois as provas digitais se apresentam, na maioria das vezes, como dinâmicas e mutáveis. Assim, há a possibilidade de se alterar as horas e data ou até mesmo torná-las imprevisíveis, embaraçando as investigações. Portanto, exigindo que o investigador realize uma investigação estruturada temporalmente, comparando vários períodos temporais.

O processo de obtenção de provas pelo investigador é essencial para a resposta do Estado sobre os cibercrimes, visto que o Brasil elegeu o sistema do livre convencimento motivado como seu sistema de apreciação de provas, conforme já demonstrado, portanto é necessário que o investigador forense capte elementos suficientes para convencer o juiz acerca da autoria do crime, além de que essas provas precisam ser válidas de acordo com o previsto pelas normas processuais penais, sob pena de contaminar toda cadeia probatória envolvida.

Além do mais, os cibercrimes apresentam uma característica própria, a extraterritorialidade, que permite a uma pessoa, independentemente, do país onde se encontre

[18] CANCELA, 2016, p. 22.

possa praticar o crime. Entretanto, as leis nacionais de cada Estado são de aplicação no seu próprio território, não acompanhando, por isso, a extraterritorialidade da *internet*.[19]

Assim, a colheita das provas digitais fica ainda mais difícil, uma vez que para obtê-las é necessário que haja cooperação jurídica internacional entre os países, o que, muitas vezes, esbarra em divergências nas legislações e na relação diplomática entre os Estados.

3.3 IDENTIFICAÇÃO DA AUTORIA

Os cibercrimes apresentam como uma de suas principais características a possibilidade de o crime ser cometido em anonimato, a ausência de espaço físico permite com que os criminosos acessem a *internet* e se utilizem de e técnicas para ocultar sua verdadeira identidade e conduta, podendo, assim, assumir qualquer identidade que não a sua.

No mundo virtual a localização de um indivíduo ocorre através de uma numeração atribuída ao internauta toda vez que uma conexão for estabelecida na *internet*, a qual denominamos endereço *IP (internet protocol).* Entretanto, os autores podem se conectar à rede através de uma conexão indireta, pela qual o internauta fica protegido e pode usufruir do anonimato on-line para acessar vários conteúdos, utilizando apenas o IP do servidor hospedeiro.[20]

Outro problema relacionado ao endereço *IP*, é que esse permite a identificação de um computador e não, efetivamente, do autor do delito. Assim, o trabalho se torna ainda mais difícil, principalmente quando os computadores estão localizados em locais públicos gerando uma dificuldade em correlacionar o sujeito que praticou o cibercrime com o computador utilizado.

---

[19] SIMAS, Diana Viveiros de. **O Cibercrime.** 2014. 170 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014. Disponível em: <https://recil.ensinolusofona.pt/bitstream/10437/5815/1/Tese%20Cibercrime%20-%20Diana%20Simas.pdf>. Acesso em: 18 out. 2022. P. 29.

[20] DIAS, Camila Barreto Andrade. **CRIMES VIRTUAIS:** As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal**.** 2014. 54 f. Monografia (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2014. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/235/5977/1/20888860.pdf>. Acesso em: 14 de nov. 2022.

4. A HISTÓRIA DOS CIBERCRIMES NO BRASIL E NO MUNDO

No Brasil, os cibercrimes são tratados como uma novidade, entretanto ao redor do mundo, principalmente na Europa, diversos países já estão a décadas empenhados em achar formas de aprimorar suas legislações de modo a combater os crimes praticados na *internet*.

Nesse sentido, trançando uma linha do tempo, podemos observar que no dia 13 de setembro de 1989 foi realizada a 428ª Reunião do Comitê dos Ministros dos Estados-Membros do Conselho da Europa, na qual foi publicada a Recomendação Nº R (89) 9[21], nesse documento foi reconhecido a característica transfronteiriça da criminalidade informática e a necessidade de aumentar a cooperação jurídica internacional para combater estes delitos, sendo assim havia a recomendação que os Estados membros do Conselho da Europa revisassem suas respectivas legislações levando em consideração o Relatório Sobre Crimes Informáticos que fora elaborado pelo Comitê Europeu.

No mesmo período, os esforços do Brasil estavam inteiramente voltados a consolidação da Constituição Federal de 1988 e a reafirmação da democracia, uma vez que o país recém superava 21 anos de uma ditadura militar (1964-1985), não havendo qualquer preocupação ou foco no combate aos cibercrimes.

Posteriormente, voltando a Europa, em 11 de setembro de 1995 foi realizado a 543ª reunião dos Ministros dos Estados Membros do Conselho da Europa onde foi publicado a Recomendação Nº R (95) 13[22], que tratava sobre à problemática de direito processual penal e tecnologia da informação.

A Recomendação Nº R (95) 13, é de extrema importância para a atividade probatória relativa aos cibercrimes, uma vez que registra o momento em que os Estados-Membros do Conselho reconheceram que as leis processuais penais tinham ausência de instrumentos investigatórios para cumprir suas tarefas, dado o contínuo desenvolvimento tecnológico do ambiente digital, principalmente quando as provas eletrônicas precisavam ser coletadas em territórios estrangeiros.

---

[21] COMMITTEE OF MINISTERS. **RECOMMENDATION Nº R (89) 9**. Disponível em: <https://rm.coe.int/09000016804f1094>. Acesso em: 16 out. 2022.

[22] COMMITTEE OF MINISTERS. **RECOMMENDATION Nº R (95) 13**. Disponível em: < https://rm.coe.int/16804f6e76>. Acesso em: 16 out. 2022.

A partir desse momento, ficou destacado a necessidade dos países membros do Conselho da Europa fortalecerem a cooperação internacional, por meio de normas processuais penais compatíveis, para as investigações de crimes ocorridos na *internet*, bem como coleta de provas eletrônicas.

Um dos pontos a Recomendação Nº R (95) 13 tratava sobre a necessidade de os países adaptarem seu ordenamento jurídico com a finalidade de coletar, preservar e apresentar as evidências eletrônicas, de forma a assegurar a integridade e autenticidade necessária para a cadeia de custódia da prova – tanto para fins processuais em seus respectivos ordenamentos jurídicos internos, quanto para fins de cooperação internacional, ou seja, a recomendação criava meios de garantir a cooperação entre os Estados-Membros do Conselho da Europa.

Desse modo, após visualizar a grandeza das problemáticas geradas com o cibercrime e da necessidade de uma cooperação internacional em um mundo cada vez mais globalizado e tecnológico, o Conselho da Europa aprova em 2001 a Convenção de Budapeste sobre o Cibercrime, a representa o grande marco para o enfrentamento dos cibercrimes, sendo considerada até os dias atuais uma referência legislativa mundial a respeito dos crimes na *internet*, sua tipificação e persecução.

A Convenção de Budapeste, apresenta dois objetivos centrais, sendo eles harmonizar os elementos do direito penal relacionados às infrações cometidas no ciberespaço e tratar da matéria processual interna nos países signatários sobre investigações dos cibercrimes, assim como as ações necessárias para obtenção da cadeia de custódia das provas eletrônicas, de forma que seja possível a implantação de um regime de cooperação internacional entre os países adeptos.

Em paralelo, no Brasil, país que não assinou à Convenção de Budapeste, há discussão no que concerne aos cibercrimes sequer havia se iniciado no poder legislativo, portanto o país não contava com legislação específica e se utilizava do Código Penal Brasileiro, ainda vigente nos dias atuais, que embora tenha recebido diversas atualizações, apresenta uma estrutura e redação original de 1940 – quarenta e oito anos, portanto, mais velhos que a Constituição Federal, e pelo menos cinco décadas antes da Revolução Digital.

Enquanto, a Constituição Federal de 1988 define em seu Artigo 5º, inciso XXXIX: "Art. 5. XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".[23]

Tal dispositivo, portanto, determina reserva legal para a tipificação, algo adotado pelo sistema jurídico romano-germânico, também conhecido como *civil law*, ao qual o Brasil adere. Desse modo, para haver constatação de delito em diversas atividades virtuais, como invasão de sistemas e acesso a dados restritos, fazia-se necessário lei específica.

Conforme afirma Medeiros, para alguém ser punido e responsabilizado penalmente, é necessário que previamente a lei descreva, minuciosamente, todos os elementos do ato considerado ilícito praticado pelo agente. No caso, determinadas condutas criminosas ocorridas mediante a utilização de sistema informatizado, dispositivo de comunicação ou rede de computadores, igualmente devem estar expressamente definidas em lei.[24]

As duas primeiras legislações específicas brasileiras para tratar dos crimes cibernéticos surgiram apenas 11 anos depois da Convenção de Budapeste, em 2012, trazendo pequenas mudanças no Código Penal de 1940, com o intuito de tipificar e tratar os crimes cibernéticos, foram elas as Leis ordinárias Nº 12.735/2012 e a Lei Nº 12.737/2012.

O resultado não foi satisfatório, uma vez que essa tipificação pouco contribuiu para o combate aos cibercrimes, que continuava em franca ascensão. Além do mais, a falta de uma legislação processual específica e a ausência de qualquer previsão referente as investigações e obtenção de provas nos cibercrimes, se apresentou como mais um dos componentes favoráveis ao fracasso do combate aos crimes praticados na *internet*, uma vez que forçou o sistema judiciário a se utilizar de ferramentas tradicionais e ineficazes para combater os delitos do campo virtual.

Sobre esse prisma, no ano de 2014 foi promulgada a Lei nº 12.965/14, também conhecida com o Marco Civil da *Internet*, que tratou em um dos seus artigos sobre a confidencialidade e a isenção do provedor, com a ressalva que que o provedor deve fornecer os

---

[23] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituição/ConstituicaoCompilado.htm>. Acesso em: 16 de out. 2022.

[24] MEDEIROS, Claudia Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos**. 2010. Disponível em: <https://docplayer.com.br/3639402-Deficiencias-da-legislacao-penal-brasileira-frente-aos-crimes-ciberneticos.html>. Acesso em: 10 out. 2022. P. 3.

registros quando judicialmente solicitados, além da imposição de responsabilidade para que eles mantivessem guardado esses dados.

Contudo, como já mencionado, a *internet* é uma terra sem fronteiras. Desse modo, abre-se a possibilidade de um crime ter um autor em um país, e uma vítima em outro, e, se cada país possuir uma legislação própria, é difícil definir a competência para apurar o crime, ou mesmo conseguir a busca pelos dados. Destarte, o legislador brasileiro descobre apenas em 2014 o que os países Europeus descobriram em 1989, a característica transfronteiriça da criminalidade informática, a qual se faz necessário um sistema de cooperação jurídica internacional para combater os cibercrimes.

Sendo assim, a combinação das dificuldades ao se tratar de competência processual para julgar os cibercrimes e há deficiência nas investigações e obtenção de provas no ciberespaço se criou um ambiente perfeito para impunidade desse tipo criminal.

Pois bem. O cenário dos cibercrimes saiu do foco nacional com esse tipo penal em constante evolução até o advento da pandemia da doença infecciosa COVID-19 e o surgimento das orientações da OMS (Organização Mundial da Saúde) para prevenção do vírus, o qual levou a um cenário de digitalização forçada em que ainda não estávamos preparados legislativamente, fazendo com que boa parte dos brasileiros tivessem implemento em sua rotina o sistema *"Home Office"*[25] como principal ferramenta de trabalho e estudo, assim impulsionando a utilização da rede mundial de *internet*.

Com o cenário de impunidade e o aumento significativo no uso da *internet*, criou-se um quadro perfeito para prática de cibercrimes, em especial aqueles baseados em *ransomware*[26], vale lembrar do recente o caso no qual a empresa JBS pagou US$ 11 milhões para não ter os dados expostos ou eliminados[27], ou o famoso caso do Ataque ao MP-SP, INSS e TJSP, onde os hackers cobravam US$ 300 por computador bloqueado.[28]

---

[25] *Home office* é uma forma de relação de trabalho na qual o colaborador atua a distância. Para isso, faz uso dos meios computacionais para produzir junto à empresa, como se estivesse presente fisicamente no escritório.

[26] O termo *ransomware,* trata-se do anglicismo utilizado para identificar a classe de malware que bloqueia os usuários dos sistemas ou restringem seu acesso, ou criptografa, ofusca, ou impede, o acesso dos arquivos, extorquindo, digitalmente, um valor específico das vítimas para a recuperação do sistema ou dos arquivos.

[27] JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. **G1.** 09 jun. 2021. Disponível em: <https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml>. Acesso em: 26 out. 2022.

[28] Acompanhe a linha do tempo do ataque hacker: MPSP, INSS e TJSP fora do ar. **Tecmundo.** 12 maio 2017. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/116639-mp-tribunal-justica-sp-desligam-maquinas-ataque-hacker.htm>. Acesso em: 19 out. 2022.

Esse quadro, pode ser identificado ao analisar o relatório do FortiGuard Labs, segundo o qual no decorrer do ano de 2020 o Brasil sofreu cerca de 8,5 bilhões de tentativas de ataques cibernéticos, enquanto no ano de 2021 o Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos, tendo um aumento de mais de 950% com relação a 2020.[29]

Nas palavras de Martins:

> "Criminosos percebendo o uso massivo da rede mundial de computadores por grande parte da população mundial procuraram, rapidamente, adaptar-se à nova realidade para cometer fraudes eletrônicas, aproveitando-se do estado de medo e ansiedade que a pandemia e a necessidade de isolamento causam as pessoas."[30]

Os prejuízos gerados são enormes, segundo o relatório *"Internet Crime Complaints Center"* realizado pela empresa de segurança digital SEON, o qual apresenta uma lista dos 10 países mais prejudicados economicamente pelo cibercrime, o Brasil ocupa a quinta colocação neste lastimável ranking, com um custo estimado em 22,5 bilhões de dólares[31].

A situação passou a exigir a adoção de medidas imediatas, vez que o cenário passou se apresentar em um contexto dramático que "beira ao caos", forçando as autoridades legislativas iniciaram uma "corrida" para o combate ao cibercrimes que iniciou-se com uma tentativa de consolidação da cultura de proteção de dados, a partir da implementação da Lei Geral da Proteção de Dados (LGPD) ao final de 2020, com a criação de uma Autoridade Nacional de Proteção de Dados (ANPD) e, também, de uma nova discussão sobre o tratamento de dados na esfera da persecução penal e de segurança pública a partir de um estudo preparatório de projeto de LGPD Penal[32].

Enquanto isso, ao redor do mundo a vasta maioria dos países signatários da Convenção de Budapeste, como Canadá, EUA, Japão, África do Sul, além dos países do continente

---

[29] Comunicados a Imprensa: Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. **FortiGuard Labs,** São Paulo, 08 fev. 2022. Disponível em: < https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em: 19 out. 2022.

[30] MARTINS, Humberto. **Seminário virtual: Criminalidade em tempo de Covid. Atuação do Sistema de Justiça.** 18 jun. 2022. Discurso. Disponível em: <https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/18062020%20discurso%20Min%20HM.pdf >. Acesso em: 26 out. 2022. P. 2.

[31] ROHALL, Pj. Global Statistics in Account Takeover Fraud for 2023. **SEON,** 22 set. 2022. Disponível em: <https://seon.io/resources/statistics-account-takeover-fraud/>. Acesso em: 18 out. 2022.

[32] Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. **STJ.** 05 nov. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx>. Acesso em: 19 out. 2022.

europeu, já contavam com entidades autônomas e independentes capazes de fazer a implementação da legislação e uma eficaz fiscalização dos agentes de tratamento de dados, além de contar com um sistema avançado de cooperação internacional que permitia uma melhor investigação e obtenção de prova dos delitos cibernéticos.

Diante deste cenário caótico e o fracasso de outras medidas adotadas, em dezembro de 2021, com o objetivo de aprimorar da legislação penal contra os crimes cibernéticos e alcançar maior celeridade para a cooperação internacional nas atividades relacionadas à persecução penal dos crimes cometidos no ambiente virtual o senado aprovou adesão do Brasil à Convenção sobre o Crime Cibernético.

Atualmente, este que é conhecido como o primeiro tratado internacional contra crimes cibernéticos. Em junho de 2021, 66 países já tinham aderido à Convenção e estimasse que seus artigos sejam usados como orientação legal em mais de 158 países.[33]

5. SUGESTÕES PARA O COMBATE A IMPUNIDADE DOS CIBERCRIMES

Os avanços no mundo digital só se tornaram possíveis graças aos investimentos na ciência e pesquisa, portanto não há como se falar em combate a cibercriminalidade e aprimoramento das investigações sem investimento.

Desde 1988, quando a rede mundial de computadores deu seus primeiros passos no Brasil, não houve preparos e investimentos por parte do Estado para combater os crimes que já vinham sendo praticados nos países que originaram a *internet*, de modo a criar um ambiente favorável a prática de crimes na rede. [34]

Como já informado, segundo o relatório *"Internet Crime Complaints Center"* [35] que ranqueia os países mais prejudicados economicamente pelo cibercrime, o Brasil ocupa a quinta

---

[33] Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético. **Senado Notícias.** 15 dez. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico>. Acesso em: 20 de nov. de 2022.

[34] CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, v. 13, jan. 2018. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em: 26 nov. de 2022.

[35] ROHALL, Pj. Global Statistics in Account Takeover Fraud for 2023. **SEON,** 22 set. 2022. Disponível em: < https://seon.io/resources/statistics-account-takeover-fraud/>. Acesso em: 18 out. 2022.

entre países mais prejudicados economicamente pelo cibercrime, com um prejuízo estimado em 22,5 bilhões de dólares.

Diante da inércia do poder público e prejuízos estratosféricos, as empresas privadas, principais afetadas, passaram a assumir a responsabilidade se tornando protagonistas do combate ao cibercrime, comprometendo grande parcela de seus recursos aos serviços de segurança cibernéticas, o que fez com que, segundo o relatório *"Internet Crime Complaints Center"* [36], esses tipos de serviço se tornassem o setor de maior e mais rápido crescimento do mercado, com receita global de US$ 86,2 bilhões.

Entretanto, o estudo denominado *"Measuring the Cost of Cybercrime"*[37] apresentou um resultado surpreendente, concluindo que a maneira mais eficiente de combate aos cibercrimes não está na antecipação do cibercrime, que já se considerou ser um feito difícil, mas sim na resposta àquele, ou seja, através da identificação dos criminosos e da sua respectiva punição.

O intuito desta colocação não está em desestimular com que as empresas privadas invistam em sua segurança na *internet*, mas sim demonstrar que há necessidade de que o Estado se retire do papel de coadjuvante no combate aos cibercrimes e exerça o *jus puniendi*, ou seja, o direito de punir.

Entre os mecanismos de combate aos crimes cibernéticos no Direito Penal a legislação, a investigação e a perícia assumem posições essenciais para o bom andamento dos processos criminais, visto que almejam a punição dos indivíduos que se utilizam do espaço cibernético para praticar crimes.

O primeiro passo para transformação deste cenário já foi dado, trata-se da assinatura e retificação da Convenção sobre os Cibercrimes, a partir do qual o Brasil se comprometeu a realizar as alterações legislativas necessária para se adequar à Convenção e se alinhar ao resto do mundo no combate aos crimes praticados na *internet*.

---

[36] Ibidem.

[37] ANDERSON, Rose; BARTON, Chris; BOHME, Rainer; CLAYTON, Richard; EETEN, Michael J.G. van; LEVI, Michael; MOORE, Tyler; SAVAGE, Stefan. Measuring the Cost of Cybercrime. In: _____. **The economics of information security and privacy.** Berlin: Springer Verlag, 2013. cap. 12, p. 265-300. Disponível em: <http://www.cs.ucr.edu/~nael/ee260/reading/cost-cybercrime.pdf>. Acesso em: 04 de nov. de 2022.

5.1 A NECESSIDADE DE ALTERAÇÕES LEGISLATIVAS.

Como já citado, é da própria natureza dos cibercrimes a realidade transfronteiriça. Dessarte, não basta que as legislações nacionais criem, isoladamente, mecanismos legais destinados a prevenir e garantir o combate contra a cibercriminalidade, mas exige a criação de instrumentos legais, de carácter universal e de cooperação internacional, de modo a poderem vir a ser implementados por todos os Estados.

Diante desse fato, a Convenção procurou, através da previsão de normas penais materiais, processuais e de cooperação internacional, harmonizar as várias legislações dos países signatários, promovendo, desta maneira, um combate mais eficaz contra a cibercriminalidade.

A maioria das medidas legislativas materiais requeridas pela Convenção já se encontram inseridas em nossa legislação penal, entretanto não apresentam a mesma abrangência e sistematização presente na Convenção, pois, como já visto, a legislação penal brasileira sobre crimes informáticos foi resultado de alterações pontuais, realizadas em momentos distintos.[38]

A maior dificuldade, em nossa análise, será a adaptação da legislação processual penal, especialmente em relação às medidas legais para rastreamento, interceptação e obtenção de dados, tema chave da Convenção. Como já comentado, existem pouquíssimas leis referentes ao tema no Brasil e se trata de tema especialmente delicado.[39]

Dessa forma, é de extrema importância que o Poder Legislativo brasileiro harmonize a nossa legislação penal nacional, baseando-se nas disposições materiais e processuais da Convenção de Budapeste, para que assim o Brasil facilite a cooperação internacional e seja incluído em uma espécie "rede internacional de contatos" que se apoiam entre si nas investigações dos crimes praticados na *internet*, denominada *24/7 Network*.

---

[38] BARBAGALO. Fernando Brandini. Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira. **Migalha**, [S.l], 2022.Disponível em: <https://www.migalhas.com.br/arquivos/2022/10/30FAAEC01AD111_Cyberciminalidade.pdf>. Acesso em: 26 out. de 2022. P. 18

[39] BARBAGALO. Fernando Brandini. Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira. **Migalha**, [S.l], 2022.Disponível em: <https://www.migalhas.com.br/arquivos/2022/10/30FAAEC01AD111_Cyberciminalidade.pdf>. Acesso em: 26 out. de 2022. P. 18

Essas alterações podem ocorrer de diferentes formas, sendo assim, pensamos, que é de extrema importância que o legislador brasileiro conheça e aproveite das experiências dos demais países signatários que já passaram por este processo de harmonização e escolha a forma mais adequada de acordo com as nossas próprias características legislativas de forma a potencializar os efeitos das mudanças legislativas que serão feitas em breve.

Na Itália, o legislador optou por realizar um conjunto de alterações no próprio Código de Processo Penal, tendo sido acrescentadas disposições processuais relativas à forma de obtenção da prova digital, adaptando assim os tradicionais meios de obtenção de prova a prova em ambiente digital, em vez de criar um regime jurídico autónomo e específico para a recolha de prova em ambiente eletrônico.[40]

Um destaque interessante da experiência italiana trata-se do cuidado do legislador em consultar alguns especialistas conceituados no assunto para que contribuísse na criação da legislação, o que ocasionou uma melhora em vários aspectos.[41]

Outro fator de grande importância adotado pela Itália que deve ser analisado pelo legislador brasileiro, considerando a nossa controvertida experiência com o tema da responsabilidade penal da pessoa jurídica, é a atribuição da adoção da responsabilidade administrativa do ente jurídico por crime de informática vinculada a atuação de seu preposto quando houver algum proveito para ela.[42]

Contudo, o legislador italiano não escapou das críticas negativas por parte da doutrina, especialmente em razão da carência de definições técnicas mais precisas, porém a avaliação da maior parte dos especialistas é positiva, uma vez que a legislação italiana sobre cibercriminalidade é abrangente e atende as diretrizes da Convenção de Budapeste, sendo considerado uma referência.[43]

---

[40] MARQUES, Maria Joana Xara-Brasil. **Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o código de processo penal.** 2014. 53 f. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade Católica Portuguesa, Lisboa, 2014. Disponível em: <https://repositorio.ucp.pt/bitstream/10400.14/17887/1/Dissertacao%20de%20Mestrado%20final%20-%20JoanaXaraBrasilMarques%20-%20Final.pdf>. Acesso em: 06 de novembro de 2022. P.39.

[41] BUCCINI, Alfonso. La Legge 48/2008 a dieci anni dalla pubblicazione. **Centro Studi Informatica Giuridica – Osservatorio di Bologna,** 5 abril de 2018**.** Disponível em: <https://www.csigbologna.it/referenze/giurisprudenza/la-legge-48-2008-a-dieci-anni-dalla-pubblicazione/>. Acesso em: 05 de nov. de 2022.

[42] BARBAGALO, 2022, p. 21.

[43] BUCCINI, 2018.

Já países como Portugal e Alemanha, optaram por englobar as disposições jurídicas relativas à cibercriminalidade em um único diploma legal.

Adentrando no direito português, temos que a Lei do Cibercrime procedeu à revogação da Lei da Criminalidade Informática no que respeita ao direito penal material, desse modo podemos dizer que o legislador português apenas realizou ajustes na legislação sobre criminalidade informática, ou seja, se limitou a proceder uma remodelação de conceitos jurídico-informáticos, acabando também por introduzir novos tipos de ilícitos criminais.[44]

Ademais, até a 2009, ano em que entrou em vigor a Lei do Cibercrime, não há que se falar no direito processual penal português um regime que regulasse, de forma específica e detalhada o modo de obtenção da prova digital, mas somente uma breve previsão no Código de Processo Penal.[45]

Há de se observar que o momento da harmonização da legislação portuguesa com a Convenção sobre o Cibercrime muito se assemelha da realidade brasileira, tanto no direito penal material como também no direito material processual.

Do ponto de vista material, o Brasil atualmente apresenta legislações penais que tipificam os crimes os cometidos na *internet*, entretanto há uma necessidade de se atualizar, introduzindo novos tipos de ilícitos criminais, tal como ocorreu em Portugal.

Já no ponto de vista processual, a semelhança entre o Brasil e Portugal está na falta de uma legislação específica para regulamentar sobretudo as investigações. Dessa forma, a experiência portuguesa e o modo como o legislador português se comportou pode ser de grande importância para o legislador brasileiro.

Além do mais, a Lei do Cibercrime implantou em Portugal o chamado Gabinete do Cibercrime, que tem como principais objetivos a coordenação, formação de magistrados do MP, interação entre os órgãos de polícia criminal e privados e acompanhamento de alguns processos, o que será revisto no tópico destinado a investigação.

[44] MARQUES, 2014, p. 15.
[45] Ibidem, p. 8.

Já em um cenário totalmente oposto ao brasileiro, ainda no ano de 1968 a Alemanha já regulava a obtenção de provas eletrônicas, através da Lei de Restrição do Segredo Postal, de Correspondência e das Comunicações à Distância e do Código de Processo Penal alemão.

Contudo, somente anos depois, através da Lei da Nova Regulamentação da Vigilância das Telecomunicações e outros Meios de Investigação Encoberta o legislador alemão atendeu à Convenção sobre o Cibercrime, aproveitando-se para aglomerar os novos aspectos relacionados com as comunicações electrónicas e criminalidade informática num só diploma legal, que trouxe como novidade a possibilidade de serem realizadas buscas online sem necessidade de despacho judicial.[46]

Sobre as mudanças geradas durante esse processo de harmonização, o maior destaque está na admissão do uso de meios ocultos de investigação, o que permitiu, por exemplo, o recurso às buscas online quando se verifique indícios de um "perigo concreto para a vida, a integridade física ou a liberdade da pessoa ou para bens da comunidade cuja ameaça afete as bases, a existência ou os fundamentos da existência do Homem."[47]

Desse modo, o legislador alemão relativizou o art. 10º da Constituição Alemã, o qual consagra o direito à inviolabilidade da correspondência e telecomunicações, e, ainda, o direito à privacidade consagrado no art. 2º da mesma lei.[48]

A adoção destas medidas ocultas de investigação vem ganhando espaço em diversos países, especialmente pela celeridade e dinamismo com que se apresenta os cibercrimes, sendo uma medida de combate com lógica eficientista e quase sempre utilizada apenas em situações emergenciais, tornando mais simples e célere o processo probatório, através do aumento dos poderes de polícia e da iniciativa policial, da redução de formalidades e mecanismos de controlo jurisdicional.[49]

No Brasil, caso houvesse a implementação de um dispositivo semelhante ao alemão, além dos dois dispositivos presentes na Constituição Alemã que também estão presente na

---

[46] SIMAS, 2014, p. 59.
[47] NEVES, Rita Castanheira. **As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova.** Coimbra: Editora, 2011, p. 104.
[48] SIMAS, 2014, p. 58.
[49] BRAZ, José Alberto Campos. **Evolução histórica da prova em processo penal do pensamento mágico à razão:** A investigação do crime organizado no estado de direito. 2017. 127 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2017. Disponível em: <https://repositorio.ul.pt/bitstream/10451/37100/3/ulfd135579_tese.pdf>. Acesso em: 12 de nov. 2022. P. 92.

Constituição Brasileira, qual seja o artigo 5º, inciso X e XII, os quais estabelecem o direito inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas e o direito à privacidade, respectivamente, infringiria também o artigo 5º, inciso LVII da CRFB, onde está consagrado o princípio da presunção de não culpabilidade, entre outros diversos dispositivos presentes no ordenamento jurídico, sendo necessário uma relativização dos mesmo.

Já no ordenamento jurídico espanhol, o legislador decidiu por inovar e regulamentar em um só artigo o regime de recolha da prova em ambiente digital, trata-se do artigo 579.º da *"Ley de Enjuiciamento Criminal".*

A constituição espanhola, assim como a brasileira, a assegura o direito à intimidade pessoal e familiar e o segredo das comunicações, em especial, as postais, telegráficas e telefônicas, exceto diante de decisão judicial.

No entanto, a doutrina espanhola relativizou esses direitos fundamentais estendendo o rol constitucional às chamadas comunicações eletrônicas. Isso se deu por meio da construção dos conceitos de comunicação em *canal abierto* e comunicação em *canal cerrado*, sendo exemplo do primeiro as páginas da web de livre acesso, fóruns, chats ou grupos de notícias não restritos, enquanto o segundo são exemplos e-mails, mensagens instantâneas ou qualquer outra forma de comunicação, incluídas aquelas que tenham seu funcionamento típico de *canal abierto,* porém operem com restrição do acesso dos participantes. Desse modo, somente as comunicações em *canal cerrado* estão protegidas pelo direito ao sigilo das comunicações.[50]

Além do mais, a "*Ley de Enjuiciamiento Criminal"* prevê que, nos casos em que houver urgência, o Ministro do Interior ou, na falta deste, o Diretor de Segurança do Estado autorize interceptação de quadrilhas armadas e elementos terroristas. Nessas hipóteses, o juiz deverá ser avisado *a posteriori*, para decidir se irá manter ou revogar a medida.[51]

---

[50] SILVA. Ricardo Sidi Machado da. **A interceptação das comunicações telemáticas no processo penal.** 2014. 266 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2137/tde-04032015-082717/publico/Ricardo_Sidi_Dissertacao_Mestrado_Integral.pdf>. Acesso em: 16 de nov. 2022.
[51] SILVA, 2014, p. 148.

5.2 INVESTIGAÇÃO CRIMINAL

Após alterações na legislação penal e processual, se faz necessário investimentos para que a lei de fato seja cumprida, é daí que se apresenta a importância do trabalho da polícia, do Ministério Público e do Judiciário.

Embora a doutrina, o Ministério Público e o Judiciário muitas vezes considerem o Inquérito policial um procedimento administrativo prescindível, é inegável a sua importância para que evite julgamentos equivocados e ações desnecessárias. Nos cibercrimes, onde há uma complexidade na obtenção das provas, temos que observar que esse instrumento é essencial não só para o desenvolvimento das investigações, mas também para a compreensão do promotor e do magistrado, de modo que deve haver, portanto, pessoas qualificadas para a busca dessas informações.

Vale lembrar, que o Código Processual Penal Brasileiro, destinou a polícia a função primordial de realizar os trabalhos de apuração dos casos concretos, de modo a embasar as denúncias e as queixas a serem promovidas pelo Ministério Público ou demais querelantes.[52]

Portanto, é função da polícia assim que chegue ao seu conhecimento a ocorrência de algum fato criminoso, realizar diligências como: comparecer ao local do crime; realizar busca e apreensão de armas, instrumentos, e outros objetos relacionados ao crime; ouvir pessoas envolvidas e testemunhas; requisitar os exames periciais necessários ao entendimento da dinâmica criminal, e praticar todos os atos essenciais para o esclarecimento dos fatos e identificação do autor do crime. [53]

Pois bem. Sendo a polícia a instituição responsável por fornecer subsídios para que o judiciário faça uma sentença completa, de modo a eliminar situações de *in dubio pro reo*, que acabem por favorecer os delinquentes, o cumprimento da lei e o consequente combate à impunidade nos cibercrimes estão diretamente condicionados a capacidade das polícias investigativas. [54]

---

[52] MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro.** 2017. 114 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade Federal do Ceára, Fortaleza, 2017. Disponível em: <https://repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf>. Acesso em: 19 de nov. 2022. P. 51.
[53] MAIA, 2017, p. 51.
[54] Ibidem, p. 52.

Desse modo, se faz necessário maiores investimentos na capacidade estrutural das polícias brasileiras para lidarem com esta modalidade criminosa praticada através da *internet*, pois, conforme já apresentado, a investigação demanda de profissionais especializados, infraestrutura e tecnologia de ponta.

Nesse sentido, o investimento em novas unidades de delegacias especializadas em crimes praticados por meio da *internet*, uma criação legislativa desenvolvida ainda em 2012, apresenta-se como uma solução. Ocorre que, embora promissora, a intenção do legislador esbarrou-se na insuficiência no número de unidades, vez que, atualmente, há apenas 18 delegacias especializadas no combate aos cibercrimes, as quais estão espalhadas por 17 estados brasileiros.[55]

Por fim, merece atenção, a solução encontrada por Portugal para impulsionar as investigações dos crimes práticos no Ciberespaço foi a criação do Gabinete do Cibercrime, o qual tem como principais objetivos a coordenação, formação de magistrados do MP, interação entre os órgãos de polícia criminal e privados e acompanhamento de alguns processos.[56]

A criação do Gabinete viabilizou os novos mecanismos de interação entre o MP e órgãos de polícia criminal e entre estes e entidades privadas, de modo que o possibilitou o desenvolvimento de canais e rotinas específicas para os processos de cibercrime, promovendo o relacionamento de todos na realização das diligências de inquérito.[57]

5.3 NECESSIDADE DE PERÍCIA ESPECIALIZADA

Na busca de combater esse cenário de crescimento de crimes cibernéticos, se faz necessário o desenvolvimento da investigação criminal, citada acima, em sintonia com a perícia criminal, uma vez que esses delitos apresentam inúmeras dificuldades na obtenção de provas válidas para o convencimento do magistrado.

---

[55] SANTOS, Maria. Delegacias virtuais: veja como denunciar crimes cibernéticos no Brasil. **Psafe**, [S.l.], 05 jul. 2022. Cibersegurança. Disponível em: <https://www.psafe.com/blog/delegacias-virtuais-veja-como-denunciar-crimes-ciberneticos-no-brasil/>. Acesso em: 14 de nov. 2022.
[56] SIMAS, 2014, p. 161.
[57] Ibidem, p.161.

Diante das dificuldades geradas pela prova digital, conforme já apresentado, para o sucesso na obtenção de provas sobre um cibercrime é necessário que haja presença de um investigador que detenha conhecimento dos princípios da Criminalística, e um perito forense digital que se utilizará de métodos científicos na coleta, validação, identificação das evidências digitais, para que se possa punir os infratores, de modo que a prova não se torne inutilizável, gerando danos a toda cadeia probatória, conforme já tratado no tópico especifico sobre os meios de provas.

Ocorre que no atual cenário, devido ao baixíssimo efetivo de peritos forenses, é comum a ausência desses profissionais em um primeiro momento, fato que pode comprometer os rumos da investigação, principalmente pelo atraso na realização dos exames periciais, diante da exigência de uma investigação célere para a punição do criminoso.

Portanto, se faz necessário investimentos com intuito de ampliar a quantidade de peritos forenses, de modo a possibilitar que as investigações sejam concluídas em tempo hábil para coleta das provas e resquícios deixados pelo infrator.

Nesse sentido, corrobora a sugestão de Maciel Colli sobre a necessidade de criação de mais divisões especializadas em computadores, mídias e meios de comunicação como um dos caminhos a serem seguidos para a solucionar alguns dos problemas relacionados a perícia.[58]

6. CONCLUSÕES

O presente artigo teve como principal objetivo analisar o desenvolvimento da atividade probatória nos cibercrimes e apresentar ao legislador brasileiro diferentes soluções encontradas por outros países durante o processo de adaptação à Convenção sobre o Cibercrime, de modo a oferecer sugestões para que essa autoridade escolha o melhor caminho observando as peculiaridades que envolve o complexo instrumento legislativo brasileiro.

[58] COLLI, Maciel. **Cibercrimes: Limites e perspectivas à investigação policial de crimes cibernéticos.** Curitiba: Juruá Editora, 2010, p. 167.

A revolução tecnologia propiciou o surgimento da *internet* que gerou diversas vantagens para a sociedade, entretanto essa ferramenta possibilitou a criação de uma nova modalidade de ilícitos, os cibercrimes.

O ciberespaço conta com uma série de características próprias que tornam esse ambiente diferente de qualquer outro já tratado pelo Direito, sendo assim o processo tradicional de investigação se tornou obsoleto. Desse modo, a primeira tentativa do legislador brasileiro foi fracassada, pois não considerou as peculiaridades da prova digital, impossibilitando que o investigador obtivesse sucesso em seu trabalho.

Sabe-se que a constituição da prova é fundamental para o convencimento do magistrado sobre a ocorrência e autoria dos fatos. Desse modo, embora o instrumento legislativo trouxesse a previsão da tipicidade dos crimes praticados na *internet*, prevalecia a impunidade, devido à falta de normas processuais, principalmente por não considerar a extraterritorialidade, o que impossibilitava a cooperação internacional.

O Brasil aderiu à Convenção sobre o Cibercrime, portanto se comprometendo a adequar o seu instrumento legislativo de forma a se harmonizar com as normas processuais de outros signatários, permitindo a cooperação internacional. Para obter maior sucesso durante esse processo de alteração, o legislador brasileiro deve aproveitar as experiências de outros países que passaram pelo mesmo processo, entretanto não esquecendo de nossas peculiaridades.

Conclui-se, ainda, que somente um ordenamento jurídico não é suficiente para acabar com a impunidade nos cibercrimes, portanto é necessário, além das alterações legislativas, um maior investimento em outros mecanismos de investigação, como a criação de delegacias especializadas e do número de peritos forenses, proporcionando assim um maior sucesso na obtenção de provas que virão a ser utilizadas no convencimento do magistrado.

REFERÊNCIAS BIBLIOGRÁFICAS:

Acompanhe a linha do tempo do ataque hacker: MPSP, INSS e TJSP fora do ar. **Tecmundo.** 12 maio 2017. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/116639-mp-tribunal-justica-sp-desligam-maquinas-ataque-hacker.htm>. Acesso em: 19 out. 2022.

ANDERSON, Rose; BARTON, Chris; BOHME, Rainer; CLAYTON, Richard; EETEN, Michael J.G. van; LEVI, Michael; MOORE, Tyler; SAVAGE, Stefan. Measuring the Cost of

Cybercrime. In: _____. **The economics of information security and privacy.** Berlin: Springer Verlag, 2013. cap. 12, p. 265-300. Disponível em: < http://www.cs.ucr.edu/~nael/ee260/reading/cost-cybercrime.pdf>. Acesso em: 04 de nov. de 2022.

Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético. **Senado Notícias.** 15 dez. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico>. Acesso em: 20 de nov. de 2022.

BARBAGALO. Fernando Brandini. Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira. **Migalha**, [S.l], 2022.Disponível em: <https://www.migalhas.com.br/arquivos/2022/10/30FAAEC01AD111_Cyberciminalidade.pdf>. Acesso em: 26 out. de 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituição/ConstituicaoCompilado.htm>. Acesso em: 16 de out. 2022.

BRAZ, José Alberto Campos. **Evolução histórica da prova em processo penal do pensamento mágico à razão:** A investigação do crime organizado no estado de direito. 2017. 127 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2017. Disponível em: <https://repositorio.ul.pt/bitstream/10451/37100/3/ulfd135579_tese.pdf>. Acesso em: 12 de nov. 2022.

BUCCINI, Alfonso. La Legge 48/2008 a dieci anni dalla pubblicazione. **Centro Studi Informatica Giuridica – Osservatorio di Bologna,** 5 abril de 2018**.** Disponível em: https://www.csigbologna.it/referenze/giurisprudenza/la-legge-48-2008-a-dieci-anni-dalla-pubblicazione/. Acesso em: 05 de nov. de 2022.

CANCELA, Alberto Gil Lima. **A prova digital**: os meios de obtenção de prova na Lei do Cibercrime. 2016. 78 f. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de Coimbra, Coimbra, 2016. Disponível em: <https://core.ac.uk/download/pdf/43589323.pdf>. Acesso em: 26 set. 2022.

CAPEZ, Fernando. **Curso de Processo Penal**. 12 ed. São Paulo: Saraiva, 2005.

COLLI, Maciel. **Cibercrimes: Limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá Editora, 2010.

COMMITTEE OF MINISTERS. **RECOMMENDATION Nº R (89) 9**. Disponível em: <https://rm.coe.int/09000016804f1094>. Acesso em: 16 out. 2022.

COMMITTEE OF MINISTERS. **RECOMMENDATION Nº R (95) 13**. Disponível em: < https://rm.coe.int/16804f6e76>. Acesso em: 16 out. 2022.

Comunicados a Imprensa: Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. **FortiGuard Labs,** São Paulo, 08 fev. 2022.

Disponível em: < https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>. Acesso em: 19 out. 2022.

Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. **STJ.** 05 nov. 2020. Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx>. Acesso em: 19 out. 2022.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito**, v. 13, jan. 2018. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em: 26 nov. de 2022.

DIAS, Camila Barreto Andrade. **CRIMES VIRTUAIS:** As inovações jurídicas decorrentes da evolução tecnológica que atingem a produção de provas no processo penal**.** 2014. 54 f. Monografia (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2014. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/235/5977/1/20888860.pdf>. Acesso em: 14 de nov. 2022

JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. **G1.** 09 jun. 2021. Disponível em: <https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml>. Acesso em: 26 out. 2022.

LAFLOUFA, Jacqueline. Hackativismo: crime cibernético ou legítima manifestação digital?. **ComCiência,** Campinas, n. 131, 2011. Disponível em: <http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542011000700006&lng=pt&nrm=iso>. Acesso em: 11 de out. 2022.

LOPES JR., Aury. **Direito processual Penal**. 14 ed. São Paulo: Saraiva, 2017.

MAIA, Teymisso Sebastian Fernandes. **Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro.** 2017. 114 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade Federal do Ceára, Fortaleza, 2017. Disponível em: <https://repositorio.ufc.br/bitstream/riufc/31996/1/2017_tcc_tsfmaia.pdf>. Acesso em: 19 de nov. 2022.

MARTINS, Humberto. **Seminário virtual: Criminalidade em tempo de Covid. Atuação do Sistema de Justiça.** 18 jun. 2022. Discurso. Disponível em: <https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/18062020%20discurso%20Min%20HM.pdf>. Acesso em: 26 out. 2022.

MARQUES, Maria Joana Xara-Brasil. **Os meios de obtenção de prova na lei do cibercrime e o seu confronto com o código de processo penal.** 2014. 53 f. Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade Católica Portuguesa, Lisboa, 2014. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/17887/1/Dissertacao%20de%20Mestrado%20final%20-%20JoanaXaraBrasilMarques%20-%20Final.pdf. Acesso em: 06 de novembro de 2022.

MEDEIROS, Claudia Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos**. 2010. Disponível em: <https://docplayer.com.br/3639402-Deficiencias-da-legislacao-penal-brasileira-frente-aos-crimes-ciberneticos.html>. Acesso em: 10 out. 2022.

MORAES, Alexandre de. **Direito Constitucional**. 27 ed. São Paulo: Atlas, 2011.

MIRABETE, Julio Fabrini. **Processo Penal**. 18 ed. São Paulo: Atlas, 2006.

MIRABETE, Julio Fabbrini. **Código de Processo Penal Interpretado**. 11 ed. São Paulo: Atlas, 2007.

NEVES, Rita Castanheira. **As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova.** Coimbra: Editora, 2011.

NUCCI, Guilherme de Souza. **Provas no Processo Penal**. 4 ed. Rio de Janeiro: Forense, 2015.

RAMOS, Armando Dias. **A Prova Digital em Processo Penal.** Lisboa: Chiado Editora, 2014.

RANGEL, Paulo. **Direito Processual Penal**. 23 ed. São Paulo. Atlas. 2015.

RODRIGUES, Benjamim Silva. **Das Escutas Telefónicas – À Obtenção da Prova (Em Ambiente) Digital**. 2 ed. Coimbra: Coimbra Editora, 2009.

RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses na investigação digital. **Revista de Engenharia e Tecnologia**, Ponta Grossa, v.2, n. 3, nov. 2010. Disponível em: <http://ri.uepg.br/riuepg/bitstream/handle/123456789/530/ARTIGO_AnaliseFerramentasForenses.pdf?sequence=1>. Acesso em: 29 set. 2022.

ROHALL, Pj. Global Statistics in Account Takeover Fraud for 2023. **SEON,** 22 set. 2022. Disponível em: <https://seon.io/resources/statistics-account-takeover-fraud/>. Acesso em: 18 out. 2022.

SANTOS, Maria. Delegacias virtuais: veja como denunciar crimes cibernéticos no Brasil. **Psafe**, [S.l.], 05 jul. 2022. Cibersegurança. Disponível em: < https://www.psafe.com/blog/delegacias-virtuais-veja-como-denunciar-crimes-ciberneticos-no-brasil/>. Acesso em: 14 de nov. 2022.

SILVA. Ricardo Sidi Machado da. **A interceptação das comunicações telemáticas no processo penal.** 2014. 266 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2137/tde-04032015-082717/publico/Ricardo_Sidi_Dissertacao_Mestrado_Integral.pdf>. Acesso em: 16 de nov. 2022.

SIMAS, Diana Viveiros de. **O Cibercrime.** 2014. 170 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014. Disponível em:

<https://recil.ensinolusofona.pt/bitstream/10437/5815/1/Tese%20Cibercrime%20-%20Diana%20Simas.pdf>. Acesso em: 18 out. 2022.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. Salvador: Jus Podivm, 2012.