REVISTA DIREITO MACKENZIE

ISSN: 23172622

CRIMES CIBERNÉTICOS: QUAL É O LUGAR DO CRIME PARA FINS DE APLICAÇÃO DA PENA E DETERMINAÇÃO DA COMPETÊNCIA JURISDICIONAL?

Fábio Ramazzini Bechara*
Dímitri Molina Flores**

RECEBIDO EM:	12.11.2019
APROVADO EM:	Convidado

* Doutor em Direito Processual Penal pela Universidade de São Paulo (USP) e mestre em Direito Processual Penal pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Professor dos Programas de Graduação e Pós-Graduação *Stricto Sensu* da Faculdade de Direito da Universidade Presbiteriana Mackenzie (UPM) e global fellow do Brazil Institute do Woodrow Wilson International Center for Scholars. Líder do grupo de pesquisa "Direito Penal Econômico e Justiça Internacional" da UPM. Promotor de Justiça em São Paulo. *E-mail*: fabio.bechara@mackenzie.br

** Graduando em Direito da Faculdade de Direito da Universidade Presbiteriana Mackenzie (UPM). Membro do grupo de pesquisa "Direito Penal Econômico e Justiça Internacional" da UPM. *E-mail*: dimitri.molina.dm@gmail.com

2019 | v. 13 | n. 2 | p. 1-21 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212928

· FÁBIO RAMAZZINI BECHARA
· DÍMITRI MOLINA FLORES

RESUMO: O objetivo do artigo é analisar, a partir da revisão bibliográfica e da legislação vigente, os critérios para delimitação do conceito de lugar do crime nos crimes cibernéticos, tendo em vista a sua relevância na definição da lei penal aplicável e na determinação do juiz natural.

PALAVRAS-CHAVE: crime cibernético; lugar do crime; lei penal; jurisdição e competência.

CYBERCRIMES: WHAT IS THE PLACE OF CRIME FOR PURPOSE AND DETERMINATION OF JURISDICTIONAL COMPETENCE?

ABSTRACT: The purpose of this article is to analyze, based on the literature review and current legislation, the criteria for delimiting the concept of place of crime in cybercrime, considering its relevance in the definition of the applicable criminal law and in the determination of the natural judge.

KEYWORDS: cybercrime; local crime; criminal law; jurisdiction and competence.

1. Introdução

O presente artigo tem o objetivo de analisar se o ordenamento jurídico brasileiro dispõe de elementos suficientes para determinar o lugar do crime nos crimes cibernéticos, seja para fins de aplicação da lei penal, seja para determinação da competência jurisdicional para o seu processo e julgamento.

Trata-se de questão atual e relevante, tendo em vista a expansão cada vez mais intensa da rede mundial de computadores, caracterizada por diferentes e dinâmicas formas de interação entre pessoas e afetação de bens jurídicos de distintas naturezas, alta rotatividade e imprecisão em relação à sua origem.

Subtrações eletrônicas de dinheiro virtual armazenados em *e-banks*, *internet banking* e criptomoedas (*bitcoins*); divulgação de mídias com conteúdo sexual referente a crianças e adolescentes; estupro virtual, pornografia de vingança; crimes contra a honra; tráfico de drogas, pessoas, armas e animais silvestres; utilização de código ma-

licioso para a invasão de dispositivos informáticos e sistemas de segurança, esses são apenas alguns exemplos de condutas prejudiciais passíveis de ser praticadas por meio de um dispositivo informático.

O resultado da conduta típica praticada em determinada localidade física do computador-meio pode se consumar em qualquer lugar do mundo, contra uma ou inúmeras vítimas, sendo certo, ainda, que seus efeitos podem se disseminar pela rede mundial de computadores inteira, alcançando número indeterminado ou mesmo indeterminável de indivíduos, de forma simultânea, alcançando assim inúmeros locais sob jurisdições nacionais distintas, mesmo que exista uma única ação criminosa.

Esse fenômeno desafia a capacidade de resposta estatal por meio da pena, tendo em vista a dificuldade de delimitação do local do crime, o que é essencial para a definição da lei penal aplicável e da competência jurisdicional.

Não constitui escopo do estudo o exame das regras de competência em relação à natureza da infração segundo o direito brasileiro, como também as eventuais de hipótese de concurso entre o crime cibernético e outros crimes, como organização criminosa, associação criminosa, entre outros.

2. Dos crimes cibernéticos: notas terminológicas

"Crimes de computador", "crimes de informática", "cibercrimes", "delitos computacionais", "crimes eletrônicos", "crimes telemáticos", "crimes informacionais" etc. (LIMA, 2011, p. 8) são algumas das inúmeras tipologias utilizadas para designar os crimes cometidos no espaço virtual, por meio de computadores ou cujo objeto é o conteúdo de um computador.

No presente artigo, optou-se pela expressão "crimes cibernéticos", que é utilizada na Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste (UNIÃO EUROPEIA, 2001), tratado internacional firmado no âmbito do Conselho da Europa.

Do gênero "crimes cibernéticos" extraem-se as espécies "próprios" (ou "fechados/exclusivamente cibernéticos") e "impróprios" (ou "abertos/mistos"), a depender do bem jurídico lesado ou da forma da prática.

Crimes cibernéticos impróprios são "condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc."

(CAIADO, 2018, p. 16). Em suma, o dispositivo informático é mero instrumento eleito pelo criminoso, que, inclusive, poderia executá-lo e consumá-lo de outra forma, sem o dispositivo.

Delitos como estelionato, ameaça, falsificação de documentos, furto mediante fraude, concorrência desleal, apologia de crime ou criminoso, racismo, tráfico de drogas, crimes contra a honra etc., ou seja, todos delitos que já existiam antes do advento "ciberespaço", praticados sem o dispositivo informático, agora podem ser praticados tanto por um quanto por outro meio.

Já os crimes cibernéticos próprios, segundo Ivette Senise Ferreira (2005, p. 261), são:

> [...] atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial pressupõem o computador como instrumento do crime, pois impossível realizarem-se sem o meio informático.

Nesse caso, o dispositivo informático é pressuposto para a realização da conduta, que não poderia ser praticada fora do ambiente virtual.

No ordenamento jurídico brasileiro, merecem destaque os seguimentos tipos penais, espécies de crimes cibernéticos próprios: 1. pornografia infantil por meio de sistema de informática (art. 241-B do Estatuto da Criança e do Adolescente – ECA), 2. corrupção de menores em salas de bate-papo da internet (art. 244-B, § 1º, do ECA), 3. violação de direitos de autor de programa de computador (art. 12 da Lei Federal n. 9.609/98), 4. inserção de dados falsos em sistema de informações (art. 313-A do Código Penal), 5. crimes contra equipamentos de voto (art. 72 da Lei Federal n. 9.504/97), 6. invasão de dispositivo informático (art. 154-A do Código Penal) e 7. interrupção ou perturbação do serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266 do Código Penal – nova redação).

Diante de um rol tão escasso de delitos, Wendt e Jorge (2012, p. 19) já alertavam que existem *ações prejudiciais atípicas*, definidas pelos autores como "condutas praticadas na/através da rede mundial de computadores que causam algum transtorno e/ou prejuízo para a vítima, porém não existe previsão penal [para punição dessas condutas]", relatando verdadeira inobservância ao princípio penal da proporcionalidade na sua

dimensão da vedação à proteção insuficiente ao bem jurídico protegido pela norma penal.

Esses delitos são costumeiramente praticados à distância ou de forma plurilocal, dada a própria natureza da conduta perpetrada por meio da rede mundial de computadores.

Em sua lição, Greco (2016, p. 232) explica que o crime à distância ocorre "quando a conduta e o resultado se desenvolvem em dois ou mais países". Está relacionado à aplicação da lei penal no espaço – norma de direito material –, isto é, com a fixação da jurisdição nacional para julgar o crime e do Estado brasileiro para reprimir a conduta. O autor explica, de outra forma, que o crime plurilocal ocorre "quando a conduta e o resultado se desenvolvem em duas ou mais comarcas, dentro do mesmo país" (GRECO, 2016, p. 232). Portanto, está relacionado à determinação interna da competência, que é o juiz natural – norma de direito processual.

A classificação é especialmente importante para a discussão acerca da delimitação territorial do delito, pois, havendo distância ou plurilocalidade, é certo que a dificuldade para determinação da jurisdição e competência é majorada e, sem estas, impossível realizar a persecução criminal dessas condutas.

3. Lugar do crime: lei penal no espaço e competência jurisdicional

3.1 Noções gerais

Uma vez que um crime foi praticado por meio de um dispositivo informático, surge ao Estado o *jus puniendi* – isto é, o direito de punir a conduta criminosa –, bem como o *jus persequendi* – direito de perseguir, investigar, processar. Os limites desse poder persecutório-punitivo estão balizados nas garantias constitucionais e legais de todo e qualquer cidadão perante o Estado, traduzidas na cláusula geral do devido processo legal, em que se insere a garantia do juiz natural.

Considerando que os crimes cibernéticos costumam ser plurilocais ou à distância, a primeira questão essencial para punição de qualquer conduta criminosa é se ela é ou não alcançada pela lei penal brasileira. A segunda questão é, uma vez que se saiba ser o crime punível segundo a lei penal brasileira, qual é o local de consumação do delito, já que por vezes há separação territorial entre autor e vítima, ação e resultado.

2019 | v. 13 | n. 2 | p. 1-21 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212928

Assim, cabe a reflexão: o que se considera lugar do crime nos crimes cibernéticos, segundo o Código Penal e o Código de Processo Penal?

A começar, o local do crime e o da infração penal são definidos a partir de um território. O Código Penal utilizou o princípio da territorialidade temperada para a aplicação da lei penal no espaço. Por princípio da territorialidade simples diz-se que a lei penal brasileira é aplicável sempre, via de regra, nos limites do território jurídico nacional. Em razão disso, o alcance da jurisdição brasileira a determinado crime cibernético está vinculado a esse crime ter sido praticado no território nacional.

De outro modo, por "temperado" deve-se entender a flexibilização subsidiária dessas regras, permitindo que o Estado brasileiro reconheça sua jurisdição sobre determinadas condutas de seu interesse para o fim de realizar a persecução penal do referido crime segundo a lei penal brasileira.

O território em que se considera praticado o crime é definido por norma de direito material trazida no art. 6º do Código Penal, que considera por local do crime tanto o local da ação ou omissão típica quanto o local do resultado obtido ou esperado. Essa prescrição revela expressamente a escolha da teoria da ubiquidade por parte do legislador em detrimento da teoria da ação ou do resultado.

Significa dizer que o Estado brasileiro, por opção política, reservou-se ao direito de punir tanto crimes cuja ação ou omissão se deu no interior do território nacional e apresentou resultado delitivo no território estrangeiro quanto condutas executadas no estrangeiro e com resultado no Brasil – o que é especialmente proveitoso para os crimes cibernéticos a distância.

Por território nacional, segundo Junqueira e Vanzolini (2014, p. 102), entende-se a junção do território real com o território por extensão. Explicam os doutrinadores que o território real corresponde à superfície terrestre, dentro dos limites das fronteiras reconhecidas, ao mar territorial brasileiro e aos seus respectivos espaços aéreos. O território por extensão, por sua vez, é a soma das embarcações e aeronaves oficiais nacionais ou privadas a serviço do governo, em qualquer lugar em que elas se encontrem, com as embarcações ou aeronaves brasileiras privadas, mas que se encontrem fora do território pertencente a qualquer Estado (leia-se: em alto-mar ou o seu espaço aéreo correspondente).

Qualquer delito praticado em quaisquer desses locais é um delito praticado no interior do território nacional e a eles é, naturalmente, aplicável a lei penal brasileira, por questão de princípio territorial simples.

Maior complexidade se tem a partir da territorialidade temperada. O legislador extrapolou o alcance da lei e jurisdição nacionais a condutas criminosas praticadas no estrangeiro, em casos excepcionais e taxativamente determinados no Código Penal. Sua consequência jurídica é a possibilidade de extraterritorialidade na aplicação da lei penal nos casos de interesse nacional.

Melhor definindo, o crime praticado no estrangeiro será punível nos termos da lei brasileira desde que satisfaça os requisitos legais do art. 7º do Código Penal. Dentre eles, para o escopo deste trabalho, importam somente os requisitos previstos nos seus incisos I, alíneas "*b*" (praticados contra o patrimônio e a fé pública da Administração Pública) e "*c*" (praticados contra a Administração Pública, por servidor público ou equiparado); e inciso II, alíneas "*a*" e "*b*" (crimes para os quais o Brasil assumiu compromisso internacional de reprimir e crimes praticados por brasileiro).

Para a persecução e punição das condutas elencadas no inciso I em sede de jurisdição nacional, o legislador não previu nenhuma condição, bastando, na seara dos crimes cibernéticos, que o crime seja praticado contra a Administração Pública. Trata-se de caso de extraterritorialidade incondicionada da lei penal brasileira, sendo a jurisdição nacional autoconfigurada para fins de persecução e punição da referida conduta.

De outra forma, o legislador determinou indiretamente para os crimes cibernéticos praticados contra particulares diversas condicionantes. Isso ocorreu porque, atendendo ao disposto no inciso II, o Brasil se obrigou internacionalmente a reprimir a delinquência cibernética[1], satisfazendo o requisito exigido, bem como é absolutamente possível a hipótese de que o autor do crime cibernético seja brasileiro. Em um e em outro caso, a jurisdição nacional alcançará a conduta quando cumprirem os requisitos do § 2º do dispositivo legal: 1. entrar o agente no território nacional; 2. ser o fato punível também no país em que foi praticado; 3. estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; 4. não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; 5. não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

Em suma, nos delitos cibernéticos a distância cuja conduta é praticada por brasileiro localizado em território estrangeiro e com advento de resultado no estrangeiro,

1 Ver convenções de Genebra, dos Direitos da Criança e do Adolescente, Estatuto de Roma, acordos bilaterais específicos etc.

2019 | v. 13 | n. 2 | p. 1-21 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212928

emerge a dificuldade de se cumprir logo o primeiro requisito. Dificilmente o agente entrará no território nacional durante a execução do crime cibernético através de dispositivo informático localizado no exterior.

O resultado será no exterior, a consumação será no exterior, o local da infração será no exterior e, segundo a previsão do código, estará fora do alcance da lei penal brasileira porque o autor não pisou em território brasileiro.

Se, de outra forma, tratar-se de conduta praticada por estrangeiro contra brasileiro, quando este for vitimado fora do Brasil, é previsão do § 3º do art. 7º do Código Penal que haja a reunião das condições anteriormente elencadas e mais dificilmente ainda o estrangeiro terá entrado no território nacional durante a prática delitiva. O resultado é no estrangeiro, sem alcance da lei brasileira.

Se, por fim, tratar-se de conduta praticada por estrangeiro contra estrangeiro vitimado no interior do território nacional, há a autorização expressa no sentido de serem condutas a que o Brasil se obrigou internacionalmente a reprimir, porém subsistirá a dificuldade de cumprir até mesmo a primeira condição determinada.

Ou seja, o rol de condições de extraterritorialidade exige requisitos praticamente inaplicáveis aos crimes cibernéticos a distância, de interesse brasileiro, especialmente quando praticados contra particulares, pois requer a condição completamente oposta à natureza dos crimes dessa espécie, que é a exigência da aproximação física entre o autor e o local do resultado criminoso, o que se revela como verdadeiro óbice à persecução penal.

A implicação do raciocínio construído aplicado aos locais do crime – regra de direito internacional – é que, nos casos em que há um particular como vítima, o Estado brasileiro estará na maior parte das vezes impedido pelo próprio Código Penal de agir em repressão à conduta praticada, embora seja de interesse persecutório, restando aguardar a jurisdição estrangeira ocupar-se dela por meio da própria lei e das próprias regras processuais. Em contrário, se for praticado contra a Administração Pública *lato sensu*, não haverá empecilho algum e automaticamente a jurisdição brasileira e a lei penal brasileira serão aplicáveis para a repressão da conduta.

Em conclusão, percebe-se que as regras de territorialidade e extraterritorialidade do Código Penal ocasionam um desequilíbrio no que tange à possibilidade de repressão por parte do Estado brasileiro aos crimes cibernéticos a distância praticados contra o particular, ao passo que a incentivam quando forem praticados contra a Administração Pública.

Resolvido o local do crime e reconhecida a jurisdição nacional sobre o fato, passa-se a analisar a determinação do local da infração – norma de interesse exclusivamente doméstico. O critério geral para a fixação da competência interna é o critério territorial trazido no texto do art. 70 do Código de Processo Penal, sendo todos os demais critérios especiais e residuais em relação a este, e aplicáveis somente quando satisfeitos os requisitos legais específicos (PACELLI, 2017, p. 267-278).

O legislador, diferentemente de quando estabeleceu as regras para determinação do local do crime, desta vez, adotou a teoria do resultado para aplicação da lei processual penal, sendo a escolha extremamente questionável para delitos praticados de forma multilocalizada, como os cibercrimes. Isso ocorreu porque, na maioria das vezes, os vestígios principais da conduta poderão estar no dispositivo utilizado pelo autor e nos seus arredores físicos, ocasião que requer a teoria da atividade para satisfatória persecução pelo próprio juízo do local da conduta, vale dizer, aquele que está perto das provas a serem produzidas. Nas demais oportunidades, os vestígios poderão se encontrar no local do dano, especialmente quando o cibercriminoso se utilizar de engenharia social presencial no local do resultado esperado, situação em que seria melhor a adoção da teoria do resultado. Por essa razão, Barreto e Brasil (2016, p. 26) explicam o seguinte:

> No caso dos delitos cibernéticos, mais apropriada é a adoção da Teoria da Ubiquidade, por ser mais completa, pois, com a volatilidade das evidências de crimes digitais, aliada ao fluxo intenso de informações, nem sempre será possível definir com clareza onde ocorreu a ação e onde houve o resultado. Em muitas ocasiões nem o criminoso nem a vítima está no local onde se consumou a ação delituosa, nem foi neste que houve o abalo social

Em síntese, assim como foi feito em relação à norma delimitadora do alcance jurisdicional (em que pese o rol de condições), a teoria da ubiquidade deveria ser a escolha para a fixação da competência jurisdicional, uma vez que crimes cibernéticos se dão no ciberespaço e não estão presos às limitações físicas do mundo material.

De toda forma, a teoria adotada e positivada pelo Código de Processo Penal foi a do resultado. Assim, o local da infração penal é o local em que se consumou o delito ou, se for o caso de crime tentado, o local em que se deu o último ato da tentativa. Essa determinação faz remissão à própria definição de crime consumado e tentado, prescrita no bojo do art. 14 do Código Penal, em que se considera o crime consumado quando "nele se reúnem todos os elementos da sua definição legal" e tentado quando o agente não

2019 | v. 13 | n. 2 | p. 1-21 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212928

consegue consumar o delito "por circunstâncias alheias à sua vontade". Conjugando os arts. 70 do estatuto processual e 14 do estatuto material, conclui-se que o território da infração penal é aquele em que ocorre o resultado da conduta criminosa, seja ele resultado naturalístico ou normativo.

Desta feita, existe conflito aparente entre as normas do art. 6º do Código Penal e do art. 70 do Código de Processo Penal. No entanto, o conflito entre as jurisdições é em todo aparente, não sendo efetivo. Conforme as lições de Brito, Fabretti e Lima (2015, p. 134-157), contrastando-se as terminologias, percebe-se que o "local do crime" é o local relacionado à prática da conduta juridicamente reprovável e penalmente relevante, levada a cabo pelo agente, bem como suas implicações e consequências. E, por essa razão, encontra-se bem alocado no direito material. Por sua vez, "local da infração" está relacionado ao local em que se considera juridicamente que houve uma violação da norma penal. E, em razão de ser onde ocorreu o desequilíbrio social, foi adotado pelo legislador como aquele em que a conduta deve ser reprimida pelo Estado – leia-se local em que o agente deve ser processado –, o que exprime verdadeira norma de caráter processual.

Guilherme Nucci (2016, p. 224) esclarece categoricamente a inexistência do efetivo conflito entre normas. Em sua lição, o art. 6º do Código Penal é norma exclusivamente de caráter penal-internacional, não interfere absolutamente na fixação da competência jurisdicional nacional. Isso ocorre porque "ela [a norma penal] não se destina à definição da competência interna, mas, sim, à determinação da competência da Justiça brasileira" (GRECO, 2016, p. 180).

A partir daí, nota-se que, nas condutas cibernéticas a distância e plurilocais, poderá existir mais de um local do crime, mais de um local de infração penal, mas obviamente deverá existir um único juiz natural para julgar aquela conduta adotada pelo seu autor.

Nesse ínterim, não é demais lembrar que, nas infrações penais classificadas analiticamente como de "consumação antecipada" (delitos formais) e de "mera conduta"[2], o local da consumação delitiva é coincidente ao da prática da conduta, de forma que o local da infração penal é o mesmo da prática da ação ou omissão. Já nas infrações penais de caráter permanente, a consumação é elastecida, deixando de ser um instante para se tornar um intervalo de tempo. Assim, a infração penal se consuma em tantos locais

2 São infrações que têm por característica a coincidência entre o momento da prática da conduta penalmente relevante e a obtenção do resultado da infração. Como nesses casos o resultado não representa uma modificação física no mundo exterior e se produz instantaneamente, foi nomeado pela doutrina como resultado normativo.

quantos forem aqueles pelos quais passou o agente durante a sua conduta criminosa. Essa situação enseja a pluralidade de foros e autoridades competentes para processar o delito, sendo necessária, para a determinação do juiz natural, a aplicação das normas subsidiárias de fixação da competência trazidos pelo legislador processual (BRITO; FABRETTI; LIMA, 2015, p. 135-137).

A maior parte dos tipos penais exclusivamente cibernéticos listados no rol apresentado traduzem-se em delitos formais ou de mera conduta. É esperado, por essa razão, que o local da infração penal nos crimes cibernéticos próprios, em regra, seja o mesmo local do dispositivo informático utilizado para praticar o crime. Enquanto isso, com relação aos delitos cibernéticos impróprios, é esperado que o local da infração penal seja análogo ao da sua prática sem o dispositivo informático – já que este é um mero meio entre tantos possíveis – e que nos delitos formais ou de mera conduta não apresente maiores problemas em sua determinação territorial.

Tendo em vista o presente raciocínio, as complicações surgem diante dos crimes cibernéticos de resultado quando praticados à distância e/ou de forma plurilocal, sejam próprios ou impróprios. Nesses, o resultado delitivo se alastra para diferentes territórios internos, para o território estrangeiro ou para ambos, de forma que a consumação pode ocorrer em qualquer lugar e sem limite de concomitância. Diante da simultaneidade de locais de consumação, eventualmente com caráter transnacional, surgem inúmeros juízos igualmente competentes e até mesmo diferentes jurisdições nacionais.

Caso a conduta seja praticada em território nacional e o resultado se dê exclusivamente no exterior, o Estado brasileiro reservar-se-á o direito de punir a referida conduta (art. 6º do Código Penal) e terá por juiz natural o magistrado brasileiro com jurisdição sobre o território em que se localizava o dispositivo informático utilizado na infração penal (art. 70, § 1º, do Código de Processo Penal).

Se houver resultado correspondente a uma ou mais vítimas no interior do território nacional, haverá multiplicidade de juízes competentes, já que haverá configuração de um ou mais resultados em diferentes territórios internos e mais o juiz competente para o resultado externo, sendo cada um deles igualmente competente.

Nesse caso, os critérios especiais do art. 69, inciso II e seguintes, do Código de Processo Penal deverão ser aplicados para realizar esse "desempate" entre os diversos órgãos judiciários concorrentes.

Na pior situação possível, haverá previsão legal e interesse dos Estados estrangeiros em perseguir e punir a conduta praticada no Brasil e com resultado no território

deles, ocasionando, além do conflito de competência entre os órgãos judiciais internos, a concorrência externa entre a jurisdição brasileira e as jurisdições nacionais, sendo cada Estado dotado de soberania para se autoproclamar com jurisdição sobre o fato e cada qual competindo para aplicar a sua lei em detrimento das demais. A partir daí, somente entendimentos na esfera política e diplomática poderiam oferecer solução ao conflito, que deverá reconhecer alguma das jurisdições como a aplicável.

3.2 Lugar do crime nos crimes cibernéticos

Os crimes cibernéticos formais e de mera conduta têm por local da infração o próprio local físico do dispositivo informático-meio utilizado na prática da conduta delitiva. Já os crimes cibernéticos materiais têm como local da infração aquele em que o resultado é obtido.

Nesses últimos, há grau crescente de complexidade conforme sejam maiores os números de vítimas e territórios em que forem configurados os respectivos resultados, pois produzem diversos órgãos judiciários igualmente competentes, dentro e fora da jurisdição nacional.

Em que pese o fato de muitos deles serem crimes formais e facilmente localizados por meio das regras expostas, aqueles que são de resultado tornam-se corriqueiramente crimes a distância ou crimes plurilocais. Isso ocorre porque podem ocasionar multiplicidade de resultados ou, ainda, ser praticados por meio de diversos autores em ação direcionada, em multiplicidade de computadores, em associação ou organização criminosa.

Assim, no caso de uma associação ou organização criminosa virtual, cujos membros estão fisicamente separados, mas são coautores ou partícipes de um mesmo crime cibernético praticado contra diversos usuários, todos os computadores envolvidos são locais do crime, sejam estes dos criminosos, dos provedores ou dos usuários vítimas (CARICATTI, 2006, p. 65-67).

No exemplo, há configuração de simultâneos resultados em diversos territórios e, consequentemente, diversos locais de consumação e diversos locais de infração penal, sendo certo que há concorrência entre as diversas jurisdições para a persecução do crime.

É cediço que o ciberespaço é um ambiente absolutamente distinto, muito além das regras tradicionais baseadas na localização geográfica. Contudo, os Estados insistem em continuar aplicando as regras jurídicas tradicionais de território para condutas

cometidas nesse novo ambiente, ao mesmo passo em que permanecem sem reconhecer que a internet está muito além do que poderia ser alcançado satisfatoriamente por elas. Essa escolha possui especial efeito em âmbito criminal, pois este é direito extremamente abrasivo à ideia de território físico e suas leis são extremamente locais em sua operação (CLOUGH, 2010, p. 405-406).

Quando se convertem exemplos da extraterritorialidade em casos de crimes cibernéticos reais, surge a dificuldade já mencionada diante das condições impostas pelo legislador para os crimes de interesse nacional e que vitimam particulares, o que poderia ser diferente. A legislação australiana penal, por exemplo, possui solução muito mais refinada e moderna, tendo adotado em seu *Criminal Code Act* previsão específica para comunicações eletrônicas. Em sua divisão 16.2., item (2), a lei penal australiana prevê qualquer emissão ou recebimento de comunicação eletrônica realizada por um indivíduo, de/para qualquer "ponto" da Austrália, como conduta parcialmente praticada em território australiano. No item seguinte (3), dilatou o alcance de "ponto" para abranger "quaisquer pontos móveis ou potencialmente móveis, ainda que na superfície, no subsolo, na atmosfera, no mar ou em qualquer outro lugar". Ou seja, trata não apenas *desktops* – máquinas fixas –, mas também de celulares, *notebooks*, *tablets* e qualquer dispositivo que possa ser utilizado para praticar cibercrimes. E, diferentemente do legislador brasileiro, não impôs sobre o Estado nenhum ônus para que seja aplicável a jurisdição australiana em tais circunstâncias.

Um outro exemplo é o Reino Unido que, nos termos do *Computer Misuse Act*, afirma sua jurisdição e alcance legislativo para as condutas que tenham ao menos um *significant link* (elo significante) com a jurisdição nacional, mesmo quando inexistir um único elemento de ocorrência no país e que o autor nunca tenha pisado naquele território. Segundo Clough (2010, p. 408-409), o *significant link* pode se configurar mesmo que o indivíduo tenha praticado a conduta criminosa no interior do seu país e que o resultado tenha se dado no interior de um outro país qualquer. Nesses termos, ocorrendo o tal elo, haverá alcance da lei britânica, ainda que a localização física nunca seja em solo britânico.

A harmonização dessas questões encontra parcial solução na Convenção de Cibercrimes, firmadas no âmbito do Conselho da Europa, e da qual o Brasil optou por não ser signatário. É a maior norma de direito internacional sobre o assunto e determinado quais condutas devem ser adotadas pelos Estados-parte, incluindo soluções sobre os conflitos de jurisdição.

2019 | v. 13 | n. 2 | p. 1-21 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v13n212928

O art. 22 da Convenção adota o princípio da territorialidade como base legitimadora para que cada Estado puna as condutas cometidas em seu território e determina que o Estado abdique do princípio da nacionalidade, segundo o qual o Estado poderá punir o seu nacional que praticar crime no exterior, em favor do Estado em que houver sido cometido o crime.

Obriga, ainda, à observância do princípio *aut dedere aut judicare*, medida anti-impunidade na qual o Estado que capturar o criminoso deverá ou processá-lo ou extraditá-lo, a depender do que for possível fazer segundo as normas internas.

A Convenção também prevê o incidente do reconhecimento da concorrência de jurisdições nacionais diversas diante do resultado de crime cibernético pulverizado pelas diversas nações. Estipula que as partes deverão realizar uma consulta para determinar qual jurisdição prevalecerá. Por motivos de eficiência e para evitar trabalhos duplicados ou incômodos desnecessários às vítimas, aos autores e às testemunhas, a Convenção determina que poderá ser acordado que um país fique com parte dos delitos e/ou da persecução penal, enquanto o outro ficará com outros, se for demonstrado como a melhor solução (UNIÃO EUROPEIA, 2001, item 235).

Diante da opção do governo federal brasileiro em não assinar a Convenção, restam as regras de direito doméstico para a determinação da competência, determinando-se primeiro o local do crime a partir da regra de direito internacional prevista no art. 5º do Código Penal, que estabelece o alcance e a forma de aplicação da lei penal brasileira no espaço, bem como dos arts. 6º e 7º, que estabelecem o conceito de território nacional e os casos de aplicação extraterritorial da lei penal brasileira.

No caso da ocorrência do concurso entre jurisdições internacionais com a nacional, o Brasil poderá utilizar as regras previstas na Convenção como parâmetro para reafirmar sua jurisdição, mas, diante da não obrigação formal a cumpri-las, é esperado que um acordo bilateral com os Estados dotados de jurisdição concorrente, em termos similares à Convenção, seja realizado para solucionar o conflito.

Mas o Brasil não é signatário nem se obrigou a cumprir as regras ali determinadas. Então, ante todo o arcabouço teórico criado, como o Estado brasileiro tem lidado com os crimes cibernéticos?

Considerando exemplos de crimes em espécie, podem-se testar as regras previstas na legislação brasileira a título de direito doméstico. Adotando como primeiro exemplo o crime de divulgação de material pornográfico infantil, previsto no art. 241-A da Lei Federal n. 8.069/90, tem-se que se trata de crime cibernético de tipo misto, podendo

ser próprio ou impróprio, mas sempre formal, cujo núcleo típico é *oferecer*, *trocar*, *disponibilizar*, *transmitir*, *distribuir*, *publicar* ou *divulgar*, e, portanto, o resultado é normativo e não naturalístico, ocorrendo *in loco* após a prática da conduta.

A jurisprudência do Superior Tribunal de Justiça e dos Tribunais Regionais Federais é unânime ao considerar que o local da consumação é o próprio local em que as imagens são divulgadas pelo autor, sendo irrelevante o local em que forem visualizadas, ou mesmo o local do provedor de acesso à rede mundial de computadores em que se encontrarem armazenadas, possuindo por *leading case* o Conflito de Competência n. 298862000.00.57047-8, cuja relatora foi a ministra Maria Thereza De Assis Moura, da Terceira Seção, julgado em 1º de fevereiro de 2008[3].

O raciocínio é idêntico para o racismo e para a injúria, pois são delitos formais praticados por meio de uma publicação, tal como o delito anteriormente analisado. O Superior Tribunal de Justiça determinou que o local de consumação do racismo praticado por meio eletrônico é o local do envio da manifestação racista[4], e o Tribunal Regional Federal da 3ª Região determinou o da injúria como o local de origem da mensagem que maculou a honra da vítima[5].

Testando para um delito de resultado, como é o caso dos crimes de furto mediante fraude e estelionato praticados por meio cibernético, há delitos cibernéticos impróprios cujas condutas típicas são, respectivamente, *subtrair* e *obter vantagem ilícita*, que pressupõem uma *res*, de propriedade ou em posse da vítima, a ser alienada pelo autor[6].

A respeito do local do crime de furto virtual, a jurisprudência nacional tem entendido que o local de consumação é o local em que o bem foi subtraído da vítima, exatamente como ocorre com o estelionato, que diverge do furto apenas em relação à forma de alienação da coisa alheia. Enquanto no furto há inversão involuntária da posse do bem furtado, no estelionato, a vítima é induzida a erro e realiza voluntariamente a inversão da posse, por meio de relação de confiança criada pelo estelionatário.

3 O entendimento exarado pela ministra foi adotado como referência pela Corte Superior e repetido nas instâncias inferiores. Cf. Superior Tribunal de Justiça. Jurisprudência. Conflitos de Competência n. 298862000.00.57047-8, 136257 2014.02.51911-6, 93739 2008.00.29800-5 e 94423 2008.00.53720-4; Tribunal Regional Federal da 4ª Região. Recurso em Sentido Estrito n. 2009.72.01.002504-0, Apelação Criminal n. 2005.71.04.005802-7; Tribunal Regional Federal da 3ª Região, Apelação Criminal n. 474930011704-91.2008.4.03.6181.

4 Cf. Conflito de Competência n. 102454 2008.02.85646-3.

5 Cf. Apelação Criminal n. 19192 0001855-71.2003.4.03.6181.

6 Aqui, resta a observação de que a alienação de *res* eletrônica não enseja a tormentosa discussão doutrinária e jurisprudencial sobre as teorias da inversão da posse e o momento de consumação. Possuem consumação instantânea, de forma que a informação com teor patrimonial que sair da esfera de proteção da vítima automaticamente estará à disposição do autor.

O exemplo clássico do furto é a subtração de dinheiro eletrônico da conta corrente da vítima, que, entendem os tribunais, consuma-se no local da agência bancária mantenedora da conta violada. Nesse sentido, o precedente do Superior Tribunal de Justiça, Conflito de Competência n. 105031 2009.00.80709, de relatoria do ministro Arnaldo Esteves Lima, da Terceira Seção, julgado em 17 de dezembro de 2009, decisão que repercutiu nas demais cortes[7].

Já a respeito do estelionato, o entendimento é idêntico, havendo inclusive súmula das cortes superiores determinando que o local do estelionato é o local em que o dinheiro se encontra quando transferido ao seu autor[8] e jurisprudência extremamente atual determinando que, quando a vítima é fraudada em uma compra, o local de consumação é aquele no qual o dinheiro sai da esfera patrimonial da vítima (agência bancária), enquanto, quando é fraudada em uma venda, o local é aquele em que a mercadoria passa a estar à disposição do criminoso[9].

Para delitos dessa natureza, resgata-se a crítica feita à adoção da teoria do resultado, pois, conforme exemplo de Barreto e Brasil (2016, p. 26), se o autor está em São Paulo e subtrai valores de conta corrente que a vítima possui em Belém, mas mora em Macapá, a atribuição da persecução penal é das autoridades locais de Belém, cidade em que não se encontrava o autor, a vítima ou potenciais testemunhas e vestígios.

Em razão disso, o Superior Tribunal de Justiça, no julgamento do Conflito de Competência n. 132.346/RS, de relatoria do ministro Rogerio Schietti Cruz, adotou tese de que o local da subtração é uma construção jurídica, ficta, pois a "administração dos valores do correntista e a sua guarda física não se equivalem", de forma que esse entendimento se estende a todos os crimes cometidos no ciberespaço. No mesmo julgamento, a Corte entendeu que a associação de criminosos virtuais que vitimaram diversas pessoas em diversos locais deve ser investigada e processada no local em que operam, pois, em que pese a associação criminosa ser delito menos gravoso que os furtos praticados, é lá e que ocorrem as deliberações da associação, ainda que outros sejam os locais de resultado das suas condutas. A seguir, apresenta-se o raciocínio do ministro:

7 Cf. Superior Tribunal de Justiça. Recurso Ordinário em *Habeas Corpus* n. 84622 2017.01.16805-0; Tribunal Regional Federal da 5ª Região, Mandado de Segurança n. 102246 2008.05.00.055091-8; Tribunal Regional Federal da 3ª Região, Conflitos de Jurisdição n. 118830044550-46.2009.4.03.0000 e 109950021890-92.2008.4.03.0000.

8 Cf. Súmula n. 244 do Superior Tribunal de Justiça.

9 Cf. Superior Tribunal de Justiça. Conflito de Competência n. 158.703/DF, julgado em 22 de agosto de 2018.

Primeiro, que o local em que foi subtraída a coisa, no caso das transferências irregulares de valores vinculados a contas bancárias, é uma construção jurídica. Observo, nesse sentido, que o endereço da agência bancária responsável pela administração dos valores do correntista não é equivalente ao local físico em que está a coisa subtraída. A administração do dinheiro e sua guarda física não se equivalem, notadamente diante da fungibilidade do dinheiro e da estrutura do sistema financeiro. Ademais, em outros crimes cibernéticos, tais como a divulgação de pornografia infantil pela internet, consideram-se consumados os delitos no lugar da ação e não no local em que se consumou a interação com o terceiro necessário à divulgação. Segundo, que, no caso de conexão dos crimes de furto mediante fraude com o crime de quadrilha, sendo este último é um crime permanente [sic], deve ser excepcionalmente processado pejo juízo do local em que foram praticadas as ações delituosas, ainda que com resultado se dê em localidade diversa. Pondero, nesse sentido, que efetivamente. segundo a teoria adotada pelo nosso Código de Processo Penal, a saber, a Teoria do Resultado, é competente para apurar a infração penal o foro do lugar de consumação do delito (art. 70, caput, do CPP). Seguindo esse critério, a definição do foro competente se dá a partir do local onde se consumou o delito mais grave. o qual, no caso concreto. seria o do furto mediante fraude (art. 155, §4°, lI, do Código Penal) já que atrelado ao delito de quadrilha ou bando (art. 288 do Código Penal). Todavia em se tratando de furto mediante fraude cometido por quadrilha de hackers no meio virtual da Internet, prevaleceria o local onde se encontra localizado o agrupamento de pessoas orientadas à prática do delito, visto que é neste lugar, onde, de fato, são planejadas e executadas as ações delituosas. em que pese o objeto subtraído situar-se virtualmente em lugar distinto. Nota-se que inúmeros serão os locais da subtração, sem, contudo, modificar-se o local de onde parte a ordem e os atos fraudulentos para a subtração de valores de contas bancárias. Deste modo, é no local onde está estabelecida a quadrilha (crime de natureza permanente) e de onde o(s) principal(is) agente(s) comanda(m) a ação criminosa – por exemplo, a disseminação de spammers, envio de programas espiões de phishíngs, monitoramento das pessoas-contas contaminadas, cooptação de "laranjas" para pagamentos de boletos e compras diversas -, que deve ser instaurada a investigação, sendo o foro daquele local o mais indicado para processar e julgar o feito com vistas à satisfação dos princípios da celeridade e efetividade. visando evitar uma tormentosa instrução distanciada da sede de onde efetivamente foi engendrada a prática criminosa. Terceiro, que, como bem exposto pelo Ministério Público Federal, o objetivo do processo penal é a punição dos agentes que cometeram crimes, de nada adiantando a instauração de diversos processos penais em que os agentes sequer serão identificados. Acrescento que, não obstante a jurisprudência consolidada do Superior Tribunal de Justiça, relativamente aos crimes de furto mediante fraude isoladamente considerados,

> a 4ª Seção do Tribunal Regional Federal da 4ª Região tem adotado o entendimento de que, no caso de crimes de furto mediante fraude conexos com o delito de quadrilha, o critério da prevenção prevalece sobre os critérios da gravidade do crime ou do local em que teria ocorrido o maior número de delitos [...].

Ou seja, houve reconhecimento jurisprudencial de que o critério territorial e sob a teoria do resultado é ineficiente para crimes cibernéticos que ocorrem além do espaço físico. Contudo, a sua aplicação só é possível mediante flexibilização e inobservância da norma processual, uma vez que o Superior Tribunal de Justiça exara entendimento contra as determinações para fixação de competência contidas no bojo do Código de Processo Penal, permitindo, mesmo sem previsão expressa, a persecução penal a partir da teoria da ubiquidade de forma estritamente teleológica, adotando o processo penal como um instrumento para realização de um fim.

Assim, resta claro que os delitos cibernéticos de resultado não obtêm solução hábil da via legislativa nos termos da atual norma processual, havendo necessidade de determinação jurisprudencial para suprir a deficiência persecutória nos crimes dessa espécie.

4. Conclusão

O ordenamento jurídico pátrio estabelece um roteiro taxativo para a fixação da competência do órgão jurisdicional para julgar qualquer delito, bem como para a aplicação da lei penal.

No caso do crime cibernético, a possibilidade de conflitos entre jurisdições estrangeiras é real, uma vez que quaisquer Estados envolvidos, seja em razão da nacionalidade da vítima ou do autor, da natureza do bem jurídico, dos efeitos, podem se julgar competentes.

A configuração desse tipo de concorrência entre os Estados dificulta especialmente a persecução criminal por parte do Estado brasileiro, pois conflitos entre as diferentes jurisdições nacionais não possuem, nem poderiam possuir, solução no direito doméstico, mas em normas de direito internacional expressas por meio de tratados, convenções, acordos bilaterais, entre outros.

Ainda que a jurisdição brasileira seja competente para julgar o crime cibernético, os atos processuais e de investigação necessários à persecução penal só podem ser

determinados pela própria jurisdição do Estado em cujo território o monopólio a ele pertence. Assim, a forma de obter a realização desses atos em território estrangeiro é por meio do instituto da cooperação jurídica internacional, procedimento envolvendo autoridades centrais e diplomáticas somadas a normas de direito internacional, sem as quais dificilmente a persecução se viabiliza.

É de se ressaltar, ainda, que o legislador nacional, quando determinou os critérios autorizadores da lei penal em caráter extraterritorial, criou condições praticamente inocorrentes em relação aos crimes cibernéticos que vitimam particulares. Sobretudo, ao exigir que o autor tenha estado no território nacional durante alguma etapa do *iter criminis*, pois, em caso contrário, o crime estará fora do alcance espacial da lei penal nacional, inexistindo até mesmo justa causa para deflagração de procedimento investigatório sumário. Com outra medida, a aplicação extraterritorial da lei penal para os crimes cibernéticos praticados contra a Administração Pública é incondicionada, bastando a configuração delitiva para ser alcançada. Resta clara a proteção deficiente dos bens jurídicos inerentes aos particulares em contraste aos inerentes à Administração Pública.

Adicione-se a isso o fato da opção política do governo brasileiro em não assinar a Convenção de Cibercrimes de Budapeste, o principal texto sobre delitos dessa natureza, deixando o Brasil à parte de uma união de esforços para a padronização da persecução penal de determinadas condutas e oferecendo solução de pacificação no concurso de jurisdições internacionais. Contudo, a Convenção, especialmente em face da sua grande adesão, poderá ser utilizada como parâmetro idôneo pelo Estado brasileiro para resolução de conflitos de jurisdição ao se deparar com concurso jurisdicional durante a persecução penal de crime cibernético de seu interesse e alcance legislativo.

A priori, a legislação aplicável é a legislação nacional, que apresenta os entraves das condições de extraterritorialidade e falta de adaptabilidade quando testada em crimes cibernéticos, pois se prende a conceitos extremamente territorialistas, enquanto o ciberespaço, local em que se desenvolvem conduta e resultado dos crimes cibernéticos, não possui delimitação física.

Assim, em que pese o crime cibernético possuir alto potencial de transnacionalidade, ao Estado brasileiro não resta sequer certeza da mera possibilidade de prosseguir à persecução criminal do crime que ultrapassar, na conduta ou no resultado, os limites fronteiriços do seu território. De forma absolutamente diversa, os cibercrimes completamente adstritos ao interior do território nacional ocasionam, no máximo, conflitos

de competência internos cuja solução é dada satisfatoriamente pelo Código de Processo Penal. No choque jurisdicional entre dois juízos competentes, utilizam-se os critérios residuais previstos no art. 69 e seguintes para a fixação da competência natural, especialmente a distribuição, prevenção, conexão e continência, havendo relativa simplicidade na determinação do juízo competente.

A incompletude normativa em relação aos crimes virtuais abre para o Poder Judiciário a possibilidade de interpretar para ocupar os vácuos regulatórios, notadamente com vistas à proteção satisfatória de bens jurídicos virtuais protegidos de forma ineficiente.

REFERÊNCIAS

BARRETO, A. G. B.; BRASIL, B. S. *Manual de investigação cibernética* **à** *luz do Marco Civil da Internet*. São Paulo: Brasport, 2016.

BRASIL. Constituição Federal de 1988. Disponível em: http://www.planalto. gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 29 jan. 2019.

BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 20 fev. 2019.

BRASIL. Decreto-Lei n 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 20 fev. 2019.

BRASIL. Lei Federal n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov. br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 24 dez. 2018.

BRITO, A. C. de; FABRETTI, H. B.; LIMA, M. A. F. *Processo Penal Brasileiro*. 3. ed. São Paulo: Atlas, 2015.

CAIADO, F.; CAIADO, M. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. *In*: MINISTÉRIO PÚBLICO FEDERAL. *Crimes cibernéticos*. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 29 jan. 2019.

CARICATTI, A. M. O local do crime no ciberespaço. *In*: BLUM, R.; BRUNO, M. G. da S.; ABRUSIO, J. C. *Manual de direito eletrônico e internet*. São Paulo: Lex, 2006.

CLOUGH, J. *Principles of cybercrime*. New York: Cambridge University Press, 2010.

FERREIRA, I. S. *Direito & internet*: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005.

GRECO, R. *Curso de direito penal*: parte especial. 13. ed. Niterói: Impetus, 2016. v. 2.

JUNQUEIRA, G.; VANZOLINI, P. *Manual de direito penal*. 2. ed. São Paulo: Saraiva, 2014.

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

NUCCI, G. de S. *Código Penal comentado*. 17. ed. Rio de Janeiro: Forense, 2017.

PACELLI, E. *Curso de Processo Penal*. 21. ed. São Paulo: Atlas, 2017.

THEODORO JÚNIOR, H. *Curso de direito processual civil*. 58. ed. Rio de Janeiro: Forense, 2017.

UNIÃO EUROPEIA. Conselho da Europa. Convenção sobre o Cibercrime. "Convenção de Budapeste". 2001. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428. Acesso em: 27 nov. 2019.

UNIÃO EUROPEIA. Conselho da Europa. Minuta explicativa da Convenção de Budapeste. 2001. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa429. Acesso em: 19 fev. 2019.

WENDT, E.; JORGE, H. V. N. *Crimes cibernéticos*: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.