# REJUB

## Revista Judicial Brasileira

### especialização em direito digital
### suplemento especial (2023)

ENFAM

Edição
Especial

https://doi.org/10.54795/RejuBEsp.DirDig.219

# A CONVENÇÃO DE BUDAPESTE E SEUS REFLEXOS SOBRE A COMPETÊNCIA PARA O PROCESSO E JULGAMENTO DOS CRIMES CIBERNÉTICOS NO BRASIL

THE BUDAPEST CONVENTION AND ITS REFLECTIONS ON THE JURISDICTION FOR THE PROCESS AND JUDGMENT OF CYBER CRIMES IN BRAZIL

**WESLEY WADIM PASSOS FERREIRA DE SOUZA**
Juiz federal do Tribunal Regional Federal da 6ª Região – TRF6. Doutor em Ciências da Comunicação pela Universidade do Vale do Rio dos Sinos – Unisinos/RS. Mestre em Direito e Instituições Políticas pela Fundação Mineira de Educação e Cultura – Fumec/MG. Especialista em Direito Penal e Processual Penal pela Faculdade de Direito do Vale do Rio Doce – Fadivale/MG. Oficial da reserva não remunerada da PMMG. Foi promotor de justiça do Estado de Minas Gerais e professor da Fadivale nas cadeiras de Direito Constitucional e Direito Processual Penal.
https://orcid.org/0000-0002-4349-2004

**RESUMO**

Neste artigo examinamos aspectos relacionados ao conceito de crimes cibernéticos e ciberespaço no contexto das mudanças desencadeadas pela digitalização, interconexão e contínua globalização das tecnologias de comunicação e informação e do crescimento exponencial da criminalidade que se utiliza da rede mundial de computadores para a prática de suas condutas. A internalização da Convenção Internacional sobre Crimes Cibernéticos, aprovada pelo Conselho da Europa em 2001, no Direito brasileiro torna-se objeto de nossa análise em especial no que tange à redefinição da competência jurisdicional para o processo e julgamento desses crimes. Porém, antes de abordarmos este ponto,

expusemos brevemente uma classificação tentativa dos delitos cujos objetos foram previstos no referido documento de direito internacional, alguns dos quais estavam presentes na legislação penal brasileira.

**Palavras-chave:** crimes cibernéticos; processual penal; Convenção de Budapeste; competência.

**ABSTRACT**

In this article we examine aspects related to the concept of cybercrime and cyberspace in the context of the changes triggered by digitalization, interconnection and continued globalization of communication and information technologies and the exponential growth of criminality that uses the world wide web to practice its conduct. The internalization of the International Convention on Cyber Crimes approved by the Council of Europe in 2001 into Brazilian law becomes the object of our analysis, especially with regard to the redefinition of criminal jurisdiction for the prosecution and judgment of these crimes. However, before approaching this point, we briefly set out a tentative classification of the crimes whose objects were foreseen in the referred document of international law.

**Keywords***:* cyber crimes; criminal procedure; Budapest Convention; jurisdiction.

**SUMÁRIO**

1 Introdução. 2 Por que preferimos a expressão “cibernético” e uma taxonomia dos crimes cibernéticos? 3 Relevância da internalização da Convenção de Budapeste na ordem jurídica brasileira. 4 Vinculação do Brasil ao tratado internacional e seus reflexos na competência

para o processo e julgamento dos crimes cibernéticos. 5 Conclusão. Referências.

## 1 INTRODUÇÃO

A difusão do uso da internet comercial que se intensifica desde a virada do milênio vem abrindo caminho para a prática de novas formas de criminalidade e novos *modus operandi* de antigas infrações. Profundas mudanças desencadeadas pela digitalização, interconexão e contínua globalização das redes informáticas foram, e ainda são, preocupações que levaram a União Europeia a buscar um tratamento uniforme em relação a esse tipo de delinquência.

Porém a gradual convergência das práticas culturais e econômicas para o ciberespaço causa desafios que extrapolam os limites de articulação dos blocos econômicos e das nações mais desenvolvidas, demandando ampliação da cooperação entre países que normalmente não têm protagonismo nas definições de normas de Direito Internacional.

De acordo com estudo divulgado em 2018, os delitos cibernéticos atingem no Brasil cerca de 62 milhões de pessoas anualmente, causando um prejuízo estimado em U$22 bilhões (Brasil, 2020).

Conforme referência contida na estratégia brasileira para segurança cibernética (Brasil, 2020), a pesquisa Cyber Review 2019 da consultoria JLT (Journal of Lightwave Technology), realizada com 200 empresas brasileiras de médio e de grande porte, apontou que 55,4% dessas empresas são totalmente dependentes do uso de tecnologia em suas atividades e que outras 35% podem ter paralizações severas diante de um problema relacionado à tecnologia. Outros dados relevantes da pesquisa são destacados a seguir: i) 80% dos entrevistados avaliaram que um incidente cibernético causaria um impacto operacional com

reflexos em toda a empresa; ii) 29% avaliaram financeiramente o que esse impacto resultaria às suas organizações; iii) 34% das empresas que responderam à pesquisa relataram ter sofrido algum tipo de incidente cibernético nos últimos doze meses; iv) 29% das empresas que sofreram ataques tiveram impactos operacionais; v) 27,8% tiveram altos custos de reconstrução sistêmica; e vi) 4% sofreram impactos de reputação frente aos clientes.

Iniciativas como a Política de Governança Digital – Decreto n. 8.638, de 15 de janeiro de 2016, a recente Estratégia Brasileira para a Transformação Digital (e-Digital) – Decreto n. 9.319, de 21 de março de 2018, e a governança no compartilhamento de dados – Decreto n. 10.046, de 9 de outubro de 2019, evidenciam o forte processo de digitalização do Governo Federal brasileiro e os parâmetros que o embasam ao longo de sua implantação, o que nos leva a perceber que os riscos inerentes à atividade privada identificados na pesquisa antes mencionada também estão presentes no setor público e que a criminalidade digital apresenta um potencial deletério extremo para toda a sociedade.

O diagnóstico da estratégia nacional de segurança cibernética de 2020 ainda menciona que:

> Grupos de *hackers* têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como: o potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional, o descrédito da população nos serviços públicos, a desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas, a desconfiança nos processos eleitorais, e o descontentamento da população com relação à administração pública (Brasil, 2020).

Nesse contexto, o estímulo à cooperação internacional em segurança cibernética, o incentivo às discussões sobre segurança

cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro e a ampliação do uso de mecanismos internacionais de combate aos crimes cibernéticos são medidas de extrema importância para a promoção dos interesses nacionais.

Diante desses desafios, pareceu-nos útil formular algumas digressões sobre a adesão brasileira à Convenção de Budapeste contra o crime cibernético, bem como sobre o estágio de internalização das disposições desse normativo internacional na ordem jurídica brasileira.

Reconhecemos que o tema é bastante amplo, podendo as abordagens serem divididas entre o direito material e o direito processual. Resolvemos, dados os limites desta comunicação acadêmica, tratar mais especificamente das eventuais alterações que a adesão do Brasil à Convenção de Budapeste pode trazer para a definição da competência para o processo e julgamento dos diversos crimes que podem ser praticados contra sistemas informáticos ou por intermédio desses sistemas, deixando para outro momento uma abordagem específica sobre a internalização de cada um dos tipos penais previstos na convenção.

Passamos, entretanto, por uma breve discussão epistemológica sobre a expressão “crimes cibernéticos” e sobre a classificação desses delitos na doutrina brasileira, antes de aportamos nas questões sobre competência que se escoram sobremaneira na verificação do estágio da jurisprudência do Superior Tribunal de Justiça – STJ sobre o tema.

## 2 POR QUE PREFERIMOS A EXPRESSÃO "CIBERNÉTICO" E UMA TAXONOMIA DOS CRIMES CIBERNÉTICOS?

Segundo Miège (2000, p. 24), "as primeiras definições da comunicação insistiam, mais ou menos, nos mecanismos que favorecem o desenvolvimento das relações humanas e, em particular, nos fenômenos de simbolização, assim como nos mecanismos de transmissão de conteúdo".

Em linhas gerais, a visão canônica sobre comunicação envolve um esquema no qual teremos um emissor, um canal, através do qual "escoará" uma mensagem (conteúdo) e um receptor, que poderá, diante da partilha de um código comum com o emissor, proceder a uma retroalimentação.

Essa proposta linear a respeito do fenômeno da comunicação permitiu críticas e aperfeiçoamentos quase sempre tendentes à redução de um fator complicador, aquilo que se convencionou chamar de ruído.

Uma das diversas propostas de aperfeiçoamento desse esquema canônico de comunicação partiu das experiências de dois engenheiros norte-americanos que trabalhavam nos laboratórios Bell na década de 1940.

Shannon e Weaver (1975) propuseram uma fórmula que permitia passar da entropia inerente aos sistemas fechados ou abertos, para a informação, eis que esta acabaria anulando ou reduzindo aquela. Daí se poder afirmar, segundo uma perspectiva matemática, que a informação[1] é a medida da redução de complexidades. A informação pode ser

[1] "Informação é um termo que designa o conteúdo do que é permutado com o mundo exterior à medida que nos adaptamos a ele e lhe aplicamos os resultados de nossa adaptação. O processo que consiste em receber e utilizar a informação é o processo que seguimos para nos adaptarmos às contingências do meio ambiente e, com eficácia, viver nesse meio" (Wiener, 1971 *apud* Miège, 2000).

apreendida como sendo a quantidade de novidades transmitidas a um receptor e que em última análise teria a capacidade de reduzir ruídos perturbadores de todos os canais de comunicação. Essa perspectiva matemática teria sido o embrião do modelo cibernético de comunicação.

Porém, em 1949, coube a Wiener (1971) estabelecer os fundamentos desse campo do conhecimento enquanto ciência dos organismos humanos e não humanos surgida da aproximação entre os comportamentos dos organismos biológicos e dos dispositivos tecnológicos, mas também como arte de governo ou de condução dos negócios do mundo. Segundo o autor, a cibernética seria "um campo inteiramente da teoria do comando e da comunicação, tanto na máquina como no animal" e se basearia na constituição de modelos que permitiriam simular o funcionamento de sistemas semi-aleatórios e no emprego de ferramentas que seriam, desde então, amplamente desenvolvidas, com base nas ideias de retroalimentação e complexidade.

A complexidade e as necessidades da vida moderna tornam mais e mais exigentes e refinados os processos de intercâmbio de informações, colocando o ser humano diante do desafio de se adaptar às novas contingências surgidas dessas inter-relações em busca de um elemento essencial à vida humana: o controle.

Nesse contexto, Wiener (1971) escolhe o termo em grego equivalente à palavra Timão – κυβερνητική – para designar todo o campo da teoria do controle e da comunicação, tanto nas máquinas quanto nos seres vivos, surgindo a cibernética.

É partindo das linhas gerais do surgimento da teoria geral dos sistemas comunicacionais (humanos e artificiais) – outra maneira de designar o que vem a ser a cibernética –, que preferimos o adjetivo cibernético para designar o tipo de criminalidade que surge do uso cada vez mais frequente de computadores e outros dispositivos

comunicacionais baseados em protocolos matemáticos para transferência de informações e simulação de realidades com ou sem conexão à rede mundial de computadores.

Não desconhecemos, entretanto, que, mesmo antes da adesão do Brasil à Convenção de Budapeste (em que a expressão crime cibernético é utilizada), os crimes dessa natureza eram conhecidos no Brasil por várias designações, tais como: crimes informáticos, crimes digitais, crimes de informática, crimes de computação, delitos de informática, abuso de computador, fraude informática etc.

Abraçamos o adjetivo cibernético não só porque ele aparece expressamente na convenção recentemente incorporada à ordem jurídica brasileira, mas também porque ele nos parece representar o gênero que alberga diversas espécies de relações ligadas ao uso de sistemas de computador para a prática das atividades que, em momento anterior a essa grande difusão do uso privado desse tipo de equipamento, eram realizadas com ferramentas não baseadas em protocolos e cálculos inerentes à linguagem de máquina.

Ressaltamos que os crimes cibernéticos sob a ótica da Convenção de Budapeste são condutas praticadas contra a confiabilidade, a integridade e a disponibilidade de sistemas de computador, ou contra outros objetos jurídicos tutelados pela legislação de um país e que tenham como instrumento essencial para sua prática um ou mais sistemas de computador.

Segundo Schimidt (2021), tais crimes podem assumir algumas classificações, a saber:

> Crimes cibernéticos impróprios: aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico da inviolabilidade da informação automatizada (dados). Exemplos de crimes informáticos impróprios podem ser calúnia (art. 138 do CP Brasileiro), difamação (art. 139 do CP Brasileiro), injúria

> (art. 140 do CP Brasileiro), todos podendo ser cometidos, por exemplo, com o envio de um *e-mail*.
> Crimes cibernéticos próprios: aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados). Como exemplo desse crime temos a interceptação telemática ilegal, prevista no art. 10 da Lei n. 9.296/96 (Lei Federal Brasileira).
> Crimes cibernéticos mistos: são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa tutelar bem jurídico de natureza diversa.
> Crimes cibernéticos mediatos ou indiretos: são os delitos-fim não informáticos que herdaram essa característica do delito-meio informático realizado para possibilitar a sua consumação.

Segundo Pinheiro (2000), citando Marco Aurélio Rodrigues, haveria os crimes cibernéticos puros, que têm por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento e a seus componentes, inclusive dados e sistemas e que, a nosso ver, tutelam juridicamente a confiabilidade, a integridade e a disponibilidade de sistemas e dados informáticos (objetos jurídicos), como, por exemplo, o art. 154-A do Código Penal – Invasão de dispositivo informático, o art. 266 do Código Penal – Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, ou o art. 298 do CP – Falsificação de cartão, todos passíveis de enquadramento nas disposições do Capítulo II, Seção 1, Título 1, da Convenção de Budapeste. Os crimes cibernéticos mistos, nos quais o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como ocorre no furto mediante fraude por meio eletrônico ou informático e na fraude eletrônica (art. 155, § 4º-B e art. 171, § 2º-A, ambos do Código Penal Brasileiro), enquadráveis no Capítulo II, Seção 1, Título 2 da Convenção de Budapeste. E os crimes cibernéticos comuns, que utilizam a internet apenas como instrumento para a realização de um delito tipificado pela lei penal, mas que poderiam ser praticados

por outros meios e instrumentos, como, por exemplo, a pornografia infantil por meio informático ou telemático (art. 241-A e 241-B, da Lei n. 8.069 de 1990), os crimes contra honra (art. 139, 140 e 141 e § 2º, do CP) e os crimes de violação de direito de autor, equivalentes ao Capítulo II, Seção 1, Títulos 3 e 4 da Convenção de Budapeste.

## 3 RELEVÂNCIA DA INTERNALIZAÇÃO DA CONVENÇÃO DE BUDAPESTE NA ORDEM JURÍDICA BRASILEIRA

A Convenção de Budapeste[2] foi criada em 2001 na capital da Hungria pelo Conselho da Europa, a fim de uniformizar o tratamento jurídico penal das condutas praticadas através dos sistemas de computação, especialmente devido ao incremento das relações levadas a efeito por meio de computadores interligados em rede e, em especial, pela difusão do uso comercial da rede mundial de computadores e pelas mudanças desencadeadas pela digitalização, interconexão e globalização das redes informáticas.

A convenção entrou em vigor em 2004, após a ratificação por cinco estados, tendo como "prioridade uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no

[2] Conforme leciona o Professor Valério Mazzuoli, os tratados e convenções internacionais são atos solenes cuja conclusão requer a observância de uma série de formalidades rigorosamente distintas e sucessivas. São quatro as fases pelas quais têm de passar os tratados solenes até sua conclusão: a) a das negociações preliminares; b) a da assinatura ou adoção, pelo Executivo; c) a da aprovação parlamentar (*referendum*) por parte de cada estado interessado em se tornar parte no tratado; e, por fim, d) a da ratificação ou adesão do texto convencional, concluída com a troca dos instrumentos que a consubstanciam. Antes da ratificação, todos os direitos e obrigações expressos no ato internacional ficam restritos às relações mútuas dos contratantes, não tendo se incorporado, ainda, no ordenamento jurídico interno desses mesmos estados. No Brasil, após a sua ratificação, o tratado, ainda, é promulgado por decreto do Presidente da República, e publicado no Diário Oficial da União. São etapas complementares adotadas pelo Estado brasileiro para que os tratados possam ter aplicabilidade e executoriedade internas (Mazzuoli, 2008 *apud* Rachel, 2010).

ciberespaço, designadamente, por meio da adoção de legislação adequada e da melhoria da cooperação internacional.

No pano de fundo da elaboração do documento normativo internacional, estavam preocupações com a crescente convergência de formas culturais e econômicas para o ciberespaço, catalisando aspectos da globalização anunciada por McLuhan (1964) desde meados do século passado.

Embora a convenção tivesse sido editada para ter abrangência no continente europeu, seu texto permitia a realização de convites para que outros países pudessem aderir. Nesse contexto, em dezembro de 2019, o Brasil foi convidado, sendo certo que a proposta tinha validade por três anos.

A adesão proporcionaria às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de tornar a cooperação jurídica internacional voltada à perseguição penal dos crimes cibernéticos mais efetiva.

Segundo Polido (2021), em 2006 era iniciado movimento no Congresso Nacional reforçando a importância de nosso Estado aderir à convenção, o Brasil havia sido convidado a integrar o grupo de países que não são membros do Conselho da Europa, como Guatemala, México, Nova Zelândia, África do Sul e Tunísia.

O histórico das propostas legislativas brasileiras a respeito do tema oscilou entre projetos inovadores e de grande presença democrática, como o que resultou no Marco Civil da Internet, e iniciativas repressivas de criminalização de usos e usuários da internet, como no Projeto de Lei n. 84/1999, apresentado pelo Senador Eduardo Azeredo (chamado também de AI-5 Digital), que criava regras para criminalizar certas condutas no ambiente digital. Entre os tipos penais, estavam os crimes de acesso e obtenção de informações em sistemas restritos, a transferência não autorizada de dados ou informações particulares e a destruição de banco de dados de terceiros.

Essa proposição normativa resultou na promulgação da Lei n. 12.735/2012, cuja maior contribuição, ainda segundo Polido (2021), teria sido a de determinar que órgãos da polícia judiciária brasileira pudessem estruturar "setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado".

Mas o que mais incomodava os especialistas era a falta de atenção das discussões congressuais no Brasil para os avanços multilaterais e a política externa de cooperação internacional em matéria digital e prevenção aos crimes cibernéticos travados no Conselho da Europa, com os procedimentos de revisão da Convenção de Budapeste de 2001.

Somente em 2021, a adesão brasileira foi ratificada pelo do Decreto Legislativo n. 37, de 16 de dezembro de 2021, tendo sido promovido o depósito dos documentos necessários junto ao Conselho da Europa em novembro de 2022, estando prevista a entrada em vigor no âmbito internacional para março de 2023.

Segundo recomendação de decisão do Conselho da Europa convocada em Bruxelas, no dia 29 de março de 2022, com a finalidade de autorizar negociações para uma convenção internacional abrangente relativa ao combate à utilização das tecnologias da informação e da comunicação para fins criminosos:

> A Convenção do Conselho da Europa sobre o Cibercrime de 2001 (Convenção de Budapeste), o primeiro tratado internacional sobre cibercriminalidade, define as infrações relacionadas com a cibercriminalidade, prevê uma série de poderes e procedimentos para investigar esse fenômeno, tais como as buscas a redes informáticas e a intercessão, e para obter provas eletrônicas seguras em relação a qualquer crime, e estabelece um quadro para a cooperação internacional. A Convenção de Budapeste está aberta a países que não são membros do Conselho da Europa, tendo a ela aderido países de todas as regiões geográficas. Até a data, 66 estados são

> partes na convenção e 14 outros países foram convidados a aderir. A convenção constitui a base da legislação para combater a cibercriminalidade em 80% dos países do mundo. A adoção do Segundo Protocolo Adicional à Convenção de Budapeste pelo Comitê de Ministros do Conselho da Europa, em 17 de novembro de 2021, demonstra que a convenção continua a ser pertinente enquanto quadro para a cooperação internacional no domínio da cibercriminalidade.
>
> A expansão das tecnologias da informação e o rápido desenvolvimento de novos sistemas de telecomunicações e de redes informáticas, bem como o uso e abuso das tecnologias para fins criminosos, também têm figurado na agenda das Nações Unidas – ONU. Em 21 de dezembro de 2010, a Assembleia Geral das Nações Unidas – AGNU adotou a Resolução n. 65/230, que solicitava à Comissão sobre Prevenção ao Crime e Justiça Penal – CPCJP a criação de um grupo de peritos intergovernamental aberto («GPI») encarregado de realizar um estudo abrangente do problema da cibercriminalidade (Comissão Europeia, 2022).

Segundo o Departamento de Cybercrime da Europol, novas formas de criminalidade têm surgido a cada dia, por isso a atualização e a ampliação territorial dos sistemas de controle e defesa criminal devem continuar em constante evolução.

Algumas formas de criminalidade conhecidas como *high tech crimes* ainda demandarão esforços para sua tipificação e adequada apuração, como, por exemplo, o Ransomware*,* que impede que os usuários acessem seus dispositivos e exige que eles paguem um resgate por meio de determinados métodos de pagamento *on-line* para recuperar o acesso; o Scareware*,* que é um falso *software* antivírus que finge escanear e encontrar ameaças de *malware*/segurança no dispositivo de um usuário para que ele pague para removê-lo; o Spyware, instalado em um computador sem o conhecimento de seu proprietário para monitorar sua atividade e transmitir as informações a terceiros; e o Adware, que exibe *banners* de publicidade ou *pop-*

*ups* que incluem código para rastrear o comportamento do usuário na internet.

Certamente a adesão à Convenção de Budapeste recoloca o Brasil no caminho das soluções com melhores evidências no contexto mundial e permite que o ambiente externo possua maior credibilidade no país.

## 4 VINCULAÇÃO DO BRASIL AO TRATADO INTERNACIONAL E SEUS REFLEXOS NA COMPETÊNCIA PARA O PROCESSO E JULGAMENTO DOS CRIMES CIBERNÉTICOS

O primeiro ponto de interesse neste tópico diz respeito à incidência da jurisdição brasileira sobre crimes praticados por pessoas que agem a partir do exterior, mas cujas condutas produzem efeitos no Brasil, situação relativamente frequente em se tratando de crimes dessa natureza. É conveniente lembrar que esse *modus operandi* permite identificarmos os chamados crimes de espaço máximo ou crimes da distância, que se distinguem dos crimes plurilocais porque nestes todo o *iter criminis* se desenrola no território nacional, embora em mais de uma comarca ou seção judiciária.

Convém acionar o art. 6º do Código Penal (Brasil, 1940) para afastar qualquer dúvida quanto à incidência da legislação brasileira, visto que se considera praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado. Ademais, ficam sujeitos à legislação brasileira, embora praticados no estrangeiro, os crimes que, por tratado ou convenção, o Brasil se obrigou a reprimir, desde que observadas as condições do § 2º do art. 7º do CP (extraterritorialidade condicionada).

Assim, mesmo que o autor da infração esteja operando no exterior, a partir do momento em que a Convenção de Budapeste entrar

em vigor, no dia 1º de março de 2023, se verificadas as condições de extraterritorialidade do Código Penal, a jurisdição brasileira se aplicará aos delitos.

Para delimitar qual é o juiz natural da persecução desses crimes é preciso responder a pelo menos mais duas perguntas, a saber: Qual a Justiça competente? Qual o juízo (foro) competente? Esta última pergunta é especialmente interessante, levando em conta as características do ambiente onde os crimes cibernéticos são praticados.

Como se sabe, esse tipo de delinquência ocorre num ambiente imaterial, muito embora possa causar prejuízos materializáveis às vítimas no mundo fenomênico. Resultado jurídico e resultado naturalístico, muitas vezes, são indissociáveis e ocorrem no mesmo momento, o que leva à imediatidade capaz de colmatar as fases finais do *iter criminis* (execução-resultado-exaurimento), trazendo complexidade para definição da competência, exemplo disso é o que ocorre nos delitos de fraude eletrônica com a finalidade de produzir vantagem econômica para o autor da conduta (Brasil, 1940, art. 171, § 2º-A, do CP).

Esse fator complicador nos permite indagar a respeito da competência para o processo e julgamento desses delitos.

Levando em conta que muitos crimes cibernéticos são ubíquos, ou seja, podem ter conduta praticada em um lugar (acesso e operação do sistema) e o resultado danoso surgindo noutro local, é preciso verificar, antes de tudo, se se trata de crime transnacional ou de espaço máximo. Dessa forma, se a conduta do agente é praticada fora do território nacional e os efeitos para a vítima são sentidos no território brasileiro (ou vice-versa), a Justiça Federal será competente para o processo e julgamento, nos termos do art. 109, V, da Constituição Federal[3],

[3] CF, art. 109. Aos juízes federais compete processar e julgar:
V – Os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no país, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (Brasil, [2016]).

levando em conta a adesão do Brasil à Convenção de Budapeste desde dezembro de 2021, por meio do Decreto Legislativo n. 37 de 21 de dezembro de 2021,[4] lembrando que, mesmo sem a publicação do decreto presidencial para a internalização do tratado, o Brasil estará obrigado na esfera internacional a realizar os compromissos nele previstos, em razão do depósito dos instrumentos confirmatórios da ratificação junto ao Conselho da Europa no dia 30 de novembro de 2022.

Esse raciocínio encontra suporte na jurisprudência do Superior Tribunal de Justiça – STJ, como se pode ver no Conflito de Competência CC n. 150629/SP, julgado em 22 de fevereiro de 2018, que, invocando a Convenção de Berna, integrada ao ordenamento jurídico nacional através do Decreto n. 75.699, de 6 de maio de 1975, e reiterada na Organização Mundial do Comércio – OMC por acordos como o Trade-Related Aspects of Intellectual Property Rights Trips – e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio – AADPIC, incorporado pelo Decreto n. 1355, de 30 de Dezembro de 1994, o Tribunal da Cidadania pela sua 3ª Seção reconheceu a competência da Justiça Federal para o processo e julgamento do crime de compartilhamento de sinal de TV por assinatura via satélite ou Card Sharing. No mesmo sentido, no CC n. 150.712-SP, relatado pelo Ministro Joel Ilan Paciornik e julgado em 10 de outubro de 2018, ficou assentado que medidas protetivas de urgência, necessárias para evitar a concretização de ameaças à mulher pelo Facebook, são de

[4] Em 11 de dezembro de 2019, conforme o item 10.3 da 1.363ª Reunião de Delegados de Ministros do Conselho da Europa, aprovou-se o convite, com prazo de cinco anos de validade, para que o Brasil pudesse aderir à Convenção sobre o Cibercrime. A adesão do Brasil à Convenção de Budapeste foi apreciada pelo Congresso Nacional por meio do Projeto de Decreto Legislativo de Acordos, Tratados ou Atos Internacionais n. 255/2021, entre junho e dezembro de 2021, dando origem à promulgação do Decreto Legislativo n. 37/2021, publicado em 21 de dezembro de 2021. A ratificação com o depósito dos documentos junto ao Conselho da Europa ocorreu em 30 de novembro de 2022, estando prevista a entrada em vigor em 1º de março de 2023 (Council of Europe, 2023).

competência da Justiça Federal, caso o agente poste mensagens a partir de sua residência no território de outro país.[5]

A competência também será da Justiça Federal se a conduta causar lesão ao patrimônio, ao serviço ou ao interesse da União, empresa pública ou entidade autárquica federal, como no caso de prejuízo concreto ao sistema de telecomunicações.

Por outro lado, a Terceira Seção do STJ (Brasil, 2022a) firmou compreensão no sentido de que a oferta de serviços de compra e venda exclusivamente de criptomoedas ou moedas virtuais não se insere na competência da Justiça Federal, por não se cuidarem de ativos regulados pelo Banco Central do Brasil ou pela Comissão de Valores Mobiliários. Nesse caso, somente se houver situação concreta em que outros interesses e serviços da União foram diretamente afetados, o processo poderá aportar na Justiça Federal (S3, CC n. 187976/RS, Min. Laurita Vaz, j. 10/8/2022, DJe. 18/8/2022). Acreditamos que esse entendimento deve ser revisto na medida em que entrar em vigor a convenção, especialmente se estivermos diante de operação que parta do exterior.

Uma vez definida a Justiça competente, deve-se passar à análise da competência territorial, ou seja, do foro competente.

Como adiantado acima, os crimes cibernéticos têm potencial para complexificar a noção de território/local do crime, eis que são cometidos num ambiente imaterial a que podemos chamar de ciberespaço.

Segundo afirma Ana Ligia (2016), a expressão ciberespaço foi usada pela primeira vez por Willian Gibson na obra Neuromancer no

[5] No caso o suposto autor das ameaças encontrava-se em território estrangeiro, uma vez que não se tinha notícia do seu ingresso no país, mas a suposta vítima teria tomado conhecimento do seu teor no Brasil. Assim ficou definido que "compete à Justiça Federal apreciar o pedido de medida protetiva de urgência decorrente de crime de ameaça contra a mulher cometido, por meio de rede social de grande alcance, quando iniciado no estrangeiro e o seu resultado ocorrer no Brasil" (Brasil, 2018a).

ano de 1984 para significar um "espaço virtual que era composto por cada computador e usuário conectado em uma rede mundial", onde as relações interpessoais poderiam ser realizadas independentemente da presença física dos envolvidos.

Segundo Lévy (1998, p. 104), a expressão refere-se ao "universo das redes digitais como lugar de encontros e de aventuras, terreno de conflitos mundiais, nova fronteira econômica e cultural". O autor complementa que o ciberespaço se conecta com diversas formas de tecnologia que têm habilidade de criar, gravar, comunicar e simular (Lévy, 1998). Assim, essa verdadeira entidade se identifica como um "*locus* do saber, uma cidade de signos, uma maneira de difusão da comunicação e de pensamento dos coletivos humanos" (Lévy, 1999), rompendo com a noção tradicional de espaço/tempo e promovendo ubiquidade e imediatidade às relações que nesse ambiente se desenvolvem.

Segundo a definição da Unesco, mencionada por Kaminiski (2002, p. 40):

> O ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e linguagens, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite à informação em trânsito ser processada e transmitida digitalmente.

Considerando que a legislação ordinária brasileira não sofreu alterações em relação à matéria de competência, mesmo que adquiramos ciência das complexidades decorrentes da verdadeira ruptura de paradigma fruto da convergência das relações humanas para o ciberespaço, temos de enfrentar as questões relacionadas com a definição do foro competente para o julgamento de crimes

cibernéticos à luz das normas que estão disponibilizadas no Código de Processo Penal.

Partindo desse pressuposto, sendo possível identificar o local onde foi consumada a infração ou praticado o último ato de execução (no caso de crime tentado), será este o foro competente, nos termos do art. 70 do CPP.

Vale alertar que, no mais das vezes, o resultado jurídico dos crimes será verificado no local em que seus efeitos forem sentidos, ainda que toda operação seja finalizada em outro local. Desse modo, se, por exemplo, uma ameaça é feita por aplicativo de WhatsApp, o local onde estiver a vítima quando receber a mensagem será o juízo competente.[6]

Se a dificuldade de definição do local do crime for insuperável em razão das peculiaridades decorrentes do seu cometimento dentro do ciberespaço, será possível acionar a regra da prevenção (art. 70, § 3º, do CPP), eis que "quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção". Observe-se que, nesse caso, não se pode invocar a competência em razão do domicílio do réu, pois não estamos diante de situação na qual não se sabe o local do crime, mas apenas diante de dúvida a respeito dele.

Assim, decidiu a Terceira Seção do STJ no Conflito de Competência CC n. 190283/RJ, julgado em 26 de outubro de 2022 e publicado no Diário da Justiça Eletrônico – DJe em 4 de novembro de 2022.

> Conforme o art. 70 do Código de Processo Penal, a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

[6] Algumas complicações decorrentes desse raciocínio podem ser afastadas pela presunção de que a vítima toma ciência das ameaças no seu domicílio.

> Especificamente quanto ao delito previsto no art. 154-A do Código Penal, o crime se consuma no momento em que o agente obtém o acesso ilícito ao dispositivo informático atacado, considerando-se como local do crime o lugar onde se encontra fisicamente o dispositivo invadido. No caso, segundo as informações existentes até o momento, os dispositivos informáticos federais objeto da invasão estavam todos situados na sede da ANATEL, em Brasília/DF, o que atrai a competência da Seção Judiciária desta Unidade Federativa. Ainda que possa haver certa dificuldade em se determinar uma localização física nos crimes cibernéticos, as regras subsidiárias de fixação da competência igualmente apontam a competência do Juízo suscitado. De fato, sendo incerto local do crime e o domicílio ou residência do autor, será competente o juiz que primeiro tomar conhecimento do fato (Brasil, 2022c).
>
> Convém lembrar que a Lei n. 14.155 de 2021 criou o parágrafo quarto do art. 70 do CPP, determinando que:
>
> [...] nos crimes previstos no art. 171 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção (Brasil, 2021).

Assim, no caso de estelionato que se dê mediante transferência de valores de uma conta bancária para outra, a competência não será definida necessariamente segundo a teoria do resultado, mas, sim, pelo inovador critério do domicílio da vítima.

O legislador, visando facilitar a reparação do dano causado ao ofendido, quebrou o paradigma segundo o qual a competência em razão do território em tema penal é definida com a finalidade de permitir uma maior eficácia da investigação atrelada às finalidades da pena eventualmente aplicada, em especial, a prevenção geral e a satisfação dos interesses da sociedade. Nesse caso, foram abandonados os critérios do local da consumação do delito, que, segundo jurisprudência

do STJ, identificava-se com a sede da conta bancária para onde tinha sido destinado o numerário fruto de fraude, conforme decidido no Conflito de Competência n. 171.455/MG, pela 3ª Seção do STJ, sob relatoria do Ministro Joel Ilan Paciornik, em 9 de dezembro de 2020 e publicado no Dje no dia 14 de dezembro de 2020 (Brasil, 2020b).

Vale lembrar que, no caso de furto praticado mediante fraude eletrônica (art. 155, § 4º–B, do CP), o STJ havia firmado jurisprudência no sentido de que, se o crime se dá por meio da rede mundial de computadores, a competência é definida pelo local onde o bem foi furtado da vítima, ou seja, na sede da conta bancária de onde o numerário é subtraído.

> PROCESSO PENAL. RECURSO EM HABEAS CORPUS. FURTO MEDIANTE FRAUDE ELETRÔNICA (VIA INTERNET). COMPETÊNCIA. CONSUMAÇÃO. AGÊNCIA DA VÍTIMA. LOCAL ONDE O BEM FOI SUBTRAÍDO. ART. 70 DO CPP. PRECEDENTES DA TERCEIRA SEÇÃO. RECURSO NÃO PROVIDO.
> 1. Hipótese em que a denúncia imputa à recorrente a prática de furto mediante fraude, através da invasão, via rede mundial de computadores, de contas bancárias mantidas em agências da Caixa Econômica Federal na cidade de Curitiba/PR.
> 2. A jurisprudência da Terceira Seção desta Corte se firmou no sentido de que a competência para o julgamento de furtos mediante fraude eletrônica (via internet) se define pelo local onde o bem foi subtraído da vítima, nos termos do art. 70, *caput*, do CPP.
> 3. Recurso não provido (Brasil, 2017).

Repita-se que, no caso de ameaças feitas pelas redes sociais ou aplicativos de mensageria, o STJ tem entendido que é competente o juízo do local em que a vítima tomou conhecimento das intimidações, pois seria nesse local onde teriam sido reunidos todos os elementos do tipo, em especial o sentimento de temor quanto à realização do mal

injusto e grave prometido pelo agressor (STJ, CC n. 156.284, S3, Rel. Min. Ribeiro Dantas, j. 28/2/2018, DJe 6/3/2018).

Por fim, vale destacar que as regras definidoras de competência têm natureza processual e, portanto, sua aplicabilidade no tempo leva em conta a data de início do processo e não a do cometimento da infração penal.

Assim, a nova definição da competência introduzida pela Lei n. 14.155, de 2021 se aplica aos processos que forem iniciados a partir de sua entrada em vigor, ou seja, a partir de 28 de maio de 2021 (Brasil, 2021).

Lembremo-nos de que, se a regra de competência territorial é alterada com o processo em curso, em razão da *perpetuatio jurisdicionis*, não há que se falar em remessa do feito para outro foro.

> CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. ESTELIONATO MEDIANTE DEPÓSITOS BANCÁRIOS. ALTERAÇÕES PROMOVIDAS PELA LEI N. 14.155/21. INAPLICABILIDADE. DENÚNCIA OFERECIDA E RECEBIDA PELO JUÍZO SUSCITADO EM MOMENTO ANTERIOR. PERPETUATIO JURISDICIONIS. CONFLITO CONHECIDO PARA DECLARAR COMPETENTE O JUÍZO SUSCITADO.
>
> 1. A competência jurisdicional é definida conforme as regras processuais vigentes no momento do oferecimento da denúncia ou da queixa-crime, sendo irrelevantes as modificações do estado de fato ou de direito ocorridas posteriormente, salvo quando suprimirem órgão judiciário ou alterarem a competência absoluta, nos termos do art. 43 do Código de Processo Civil, c.c. o art. 3º do Código de Processo Penal.
>
> 2. A Lei n. 14.155/21, ao criar hipótese específica de competência territorial para julgamento dos crimes de estelionato praticado mediante depósito, transferência de valores ou cheque sem provisão de fundos em poder do sacado ou com o pagamento frustrado, não suprimiu órgão judiciário nem alterou competência absoluta. Assim, a alteração legislativa não modifica a competência anteriormente fixada pelo oferecimento da denúncia.

> 3. Conflito conhecido para declarar competente o JUÍZO DE DIREITO DA 5ª VARA CRIMINAL DE FORTALEZA/CE (Suscitado) (Brasil, 2022b).

## 5 CONCLUSÃO

Como se tentou deixar claro nas linhas anteriores, muito embora a ordem jurídica brasileira contemple preocupação com os crimes cibernéticos há mais de uma década, a adesão do Brasil à Convenção de Budapeste terá potencial para trazer importantes reflexos para a rotina de persecução desse tipo de delinquência pelas instituições brasileiras.

As questões sobre competência são só alguns dos muitos reflexos que serão sentidos pelos operadores do direito no seu dia a dia.

Acreditamos que a cooperação internacional nesta matéria também trará reflexos positivos na diminuição dessa criminalidade, mas esperamos ter oportunidade de analisar o tema no futuro, quando as observações empíricas nos puderem trazer elementos mais consistentes à observação.

## REFERÊNCIAS

ANA LIGIA. **Entenda o que é ciberespaço e como surgiu a expressão**. [*S. l.*]: Estudo prático, 18 out. 2016. Disponível em: https://www.estudopratico.com.br/entenda-o-que-e-ciberespaco-e-como-surgiu-a-expressao/. Acesso em: 12 fev. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 fev. 2023.

BRASIL. **Decreto n. 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF: Presidência da República, 2020a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 11 fev. 2023.

BRASIL. **Decreto-Lei n. 2.848 de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art154a. Acesso em: 10 fev. 2023.

BRASIL. **Decreto-Lei n. 3.689 de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689.htm. Acesso em: 10 fev. 2023.

BRASIL. **Lei 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. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 fev. 2023.

BRASIL. **Lei n. 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei n. 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato de 24 de julho de 1991. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 10 fev. 2023.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência n. 150.712 - SP (2017/0014052-4)**. Conflito negativo de competência. Juízo estadual x juízo federal. Ameaças de ex-namorado a mulher via Facebook. Medidas protetivas de urgência [...]. Relator: Min. Joel Ilan Paciornik, 10 de outubro de 2018a. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700140524&dt_publicacao=19/10/2018. Acesso em: 19 dez. 2022.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência n. 156.284 - PR (2018/0008775-5)**. Conflito de competência. Crime de ameaça praticado por WhatsApp e Facebook. Âmbito de aplicação da Lei Maria da Penha. Delito formal. Consumação no local onde a vítima conhece das ameaças. Conflito de competência conhecido. Declarada a competência do juízo suscitado [...]. Relator: Min. Ribeiro Dantas, 28 de fevereiro de 2018b. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201800087755&dt_publicacao=06/03/2018. Acesso em: 12 fev. 2023.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência n. 171455 - MG (2020/0075540-3)**. Conflito negativo de competência. Inquérito policial. Estelionato em tese praticado via internet. Pagamento efetuados pela vítima mediante boleto bancário falso. Numerário creditado na conta corrente do suposto estelionatário. Competência do local em que se auferiu a vantagem indevida: local da conta para a qual foi transferido o dinheiro. Relator: Min. Joel Ilan Paciornik, 9 de dezembro de 2020b. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202000755403&dt_publicacao=14/12/2020. Acesso em: 10 fev. 2023.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência n. 187.976 - RS (2022/0127313-5)**. Conflito de competência. Processual penal. Investimentos em criptomoedas. Prestação de serviços de câmbio. Recursos captados em moeda nacional. Oferta pública na internet e em redes sociais. Contrato de adesão. Atuação irregular como instituição financeira. Competência federal. Conflito conhecido para declarar competente o juízo federal suscitante [...]. Relatora: Ministra Laurita Vaz, 10 de agosto de 2022a. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201273135&dt_publicacao=18/08/2022. Acesso em: 19 dez. 2022.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência n. 193.198 - SP (2022/0368950-6)**. Conflito negativo de competência. Processual penal. Estelionato mediante depósitos bancários. Alterações promovidas pela Lei n. 14.155/21. Inaplicabilidade. Denúncia oferecida e recebida pelo juízo suscitado em momento anterior. Perpetuatio jurisdicionis. Conflito conhecido para declarar competente o juízo suscitado [...]. Relatora: Min. Laurita Vaz, 14

de dezembro de 2022b. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202203689506&dt_publicacao=19/12/2022. Acesso em: 19 dez. 2022.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência n. 190.283 - RJ (2022/0227388-6)**. Conflito negativo de competência. Ataques contra a agência nacional de telecomunicações - ANATEL. Inquérito policial. Invasão de dispositivo informático. Local de consumação do crime. Localização física dos dispositivos invadidos. Relatora: Ministra Laurita Vaz, 26 de outubro de 2022c. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202202273886&dt_publicacao=04/11/2022. Acesso em: 19 dez. 2022.

BRASIL. Superior Tribunal de Justiça (5. turma). **Recurso Ordinário em Habeas Corpus 84622/PR**. Processo penal. Recurso em Habeas Corpus. Furto mediante fraude eletrônica (via internet). Competência [...]. Relator: Min. Ribeiro Dantas, 17 de agosto de 2017. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201701168050&dt_publicacao=28/08/2017. Acesso em: 19 dez. 2022.

CARDOZO, Alexandro Gianes. **Competência nos crimes cibernéticos**. [*S. l.*]: JusBrasil, 2017. Disponível em: https://agianes.jusbrasil.com.br/artigos/514359859/competencia-nos-crimes-ciberneticos. Acesso em: 17 fev. 2023.

COMISSÃO EUROPEIA. **Recomendação de Decisão do Conselho**. Que autoriza as negociações para uma convenção internacional abrangente relativa ao combate à utilização das tecnologias da informação e da comunicação para fins criminosos. Bruxelas: COM, 29 Mar. 2022.

Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52022PC0132. Acesso em: 19 fev. 2023.

CONSELHO DA EUROPA. **Convenção sobre o cibercrime**. Budapeste: CoE, 2011. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 4 dez. 2022.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Trad.: Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 185**. Europe, CoE, 2023. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Acesso em: 12 fev. 2023.

KAMINSKI, Omar. A informática jurídica, a juscibernética e a arte de governar. **Revista Consultor Jurídico**, [*s. l.*], 17 jul. 2002. Disponível em: http://www.conjur.com.br/2002-jul-17informatica_juridica_juscibernetica_arte_governar. Acesso em: 12 fev. 2023.

LÉVY, Pierre. **A inteligência coletiva**: por uma antropologia do ciberespaço. Trad. L. P. Rouanet. **São Paulo: Loyola**, 1998.

LÉVY, Pierre. **Cibercultura**. Trad. C. I. da Costa. São Paulo: Editora 34, 1999.MAZZUOLI, Valério de Oliveira. **Direito internacional público**: parte geral. 4. ed. São Paulo: Revista dos Tribunais, 2008.

MCLUHAN, Marshall. **Understanding Media**. Londres: Routledge, 1964.

MCLUHAN, Marshall. **A galáxia de Gutenberg**: a formação do homem tipográfico. 2. ed. Trad. Leônidas Gontijode Carvalho & Anísio Teixeira; apres. Anísio Teixeira. **São Paulo:** Editora Nacional, 1977.

MIÈGE, Bernard. **O pensamento comunicacional**. Trad. Guilherme João de Freitas Teixeira. Petrópolis: Vozes, 2000.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. Revista Jus Navigandi, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: https://jus.com.br/artigos/1830. Acesso em: 18 fev. 2023.

POLIDO, Fabricio Bertini Pasquot. Por que o Brasil deve urgentemente aderir à Convenção de Budapeste. **Consultor Jurídico**, [*s. l.*], 5 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-05/polido-brasil-urgentemente-aderir-convencao-budapeste?imprimir=1. Acesso em: 14 fev. 2023.

RACHEL, Andrea Russar. **Quais são as quatro fases a que se submetem os tratados e convenções internacionais**? [*S. l.*]: Rede de Ensino Luiz Flávio Gomes, 2009. Disponível em: https://lfg.jusbrasil.com.br/noticias/2064249/quais-sao-as-quatro-fases-a-que-se-submetem-os-tratados-e-convencoes-internacionais-andrea-russar-rachel. Acesso em: 17 fev. 2023.

ROSA, Fabrízio. **Crimes de informática**. Campinas: Bookseller, 2002.

SCHMIDT, Guilherme. **Crimes cibernéticos**. [*S. l.*]: Jusbrasil, 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: 13 fev. 2023.

SHANNON, Claude; WEAVER, Warren. **Theorie mathématique de la communication**. Paris: CEPL, 1975.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

WIENER, Norbert. **Cibernética e sociedade**. Paris: Bourgeois, 1971.