A CONVENÇÃO DE BUDAPESTE SOBRE OS CRIMES CIBERNÉTICOS FOI PROMULGADA, E AGORA?

THE BUDAPEST CONVENTION ON CYBERCRIMES WAS ENACTED, WHAT NOW?

Ana Maria Lumi Kamimura Murata
Doutora e Mestre em Direito Penal pela USP.
Bacharel em Direito pela UFPR. Advogada.
Link Lattes: http://lattes.cnpq.br/8320271873151749
ORCID: https://orcid.org/0000-0003-4182-4754
anammurata@gmail.com

Paula Ritzmann Torres
Doutoranda e Mestre em Direito Internacional pela USP. Bacharel em Direito pela UFPR e em Relações Internacionais pela Unicuritiba. Advogada.
Link Lattes: http://lattes.cnpq.br/6742580278458464
ORCID: https://orcid.org/0000-0002-0849-9913
paula.r.torres@usp.br

Resumo: Com a promulgação da Convenção sobre o Crime Cibernético (Decreto 11.491/2023), o Brasil assumiu novas obrigações internacionais no combate ao crime cibernético. O artigo foca em três aspectos penais e processuais da Convenção (tipificação de cibercrimes, responsabilidade penal da pessoa jurídica e cooperação jurídica internacional para a obtenção de provas digitais), que, por sua natureza inovadora, demandam reflexão sobre as medidas a serem adotadas pelo Estado para sua implementação e compatibilidade com a ordem jurídica brasileira.

Palavras-chave: Convenção de Budapeste; Crimes cibernéticos; Responsabilidade penal da pessoa jurídica; Cooperação jurídica internacional.

Abstract: With the enactment of the Cybercrime Convention (Decree 11,491/2023), Brazil assumed new international obligations in the fight against cybercrime. The article focuses on three criminal and procedural aspects of the Convention (typification of cybercrimes, criminal liability of legal entities, and international legal cooperation for obtaining digital evidence), which, due to their innovative nature, demand reflection on the measures to be adopted by the State for its implementation and compatibility with the Brazilian legal system.

Keywords: Budapest Convention; Cybercrimes; Criminal liability of legal entities; International legal cooperation.

1. Introdução

A criminalidade cibernética se tornou uma preocupação do Conselho da Europa na década de 1980, que foi evidenciada com a adoção das recomendações sobre crimes envolvendo computadores e tecnologia da informação no processo criminal. A seguir, na década de 1990, o Conselho criou um comitê para elaborar um *draft* de convenção sobre os crimes cibernéticos, buscando conferir segurança jurídica e, ao mesmo tempo, ser adaptável à constante evolução tecnológica (COUNCIL OF EUROPE, 2021a).

Como resultado, a Convenção sobre o Crime Cibernético foi aberta para assinatura em 2001, em Budapeste. O texto convencional conta com três capítulos, o primeiro deles estipulando conceitos para a mútua compreensão e o desenvolvimento dos trabalhos; o segundo sobre as medidas a serem adotadas nas jurisdições nacionais, subdividido em três seções (Direito Penal, Direito Processual e Jurisdição); e o terceiro sobre cooperação internacional, com principiologia e mecanismos de assistência jurídica internacional.

Passados mais de vinte anos desde sua entrada em vigor na ordem internacional, a Convenção se mantém relevante e atual, tendo sido ratificada por 68 Estados, membros e não membros do Conselho da Europa. O Brasil ratificou a Convenção em 2022 e a promulgou internamente com o Decreto 11.491/2023.

A adesão do Brasil à Convenção de Budapeste era necessária. Com a globalização e o desenvolvimento da informática, houve um aumento do número de usuários da *internet* e foram criadas novas formas de praticar crimes, com diferentes bens jurídicos, aumentando o número de vítimas e a dimensão do dano. Ademais, a dispersão das informações e da geolocalização dos autores agregou complexidade à persecução penal, na obtenção de provas, na definição de jurisdição e na individualização da responsabilidade.

Contudo a assunção de obrigações internacionais para o combate ao cibercrime não basta, sendo necessário adotar medidas internas em matéria penal e processual penal para torná-las efetivas. O objetivo deste artigo é apenas chamar atenção para três aspectos da Convenção que suscitam reflexão sobre a forma de implementação e compatibilidade com a ordem jurídica brasileira: a tipificação de cibercrimes; a responsabilidade penal da pessoa jurídica por crimes cibernéticos e a cooperação jurídica internacional para a obtenção de provas digitais.

2. Cibercrimes na legislação brasileira

O que se quer expressar ao falar de cibercrimes ou criminalidade cibernética? Essa não é uma terminologia legal, e sim um termo casual. Para ser *cyber* não basta estar relacionado a um computador, mas sim conectado à rede. Por esse motivo, nos Estados Unidos, Reino Unido, Canadá e Austrália, utiliza-se a classificação de delitos *cyber*-capacitados e *cyber*-dependentes; o primeiro grupo contemplando aqueles cometidos por meio da tecnologia da

informação e comunicação (TIC) e que a tem como alvo (*hacking*, *malware*, pirataria digital etc.), e o segundo que pode ser cometido sem o uso de TIC, mas que, quando a utiliza, há uma mudança significativa de escala e alcance (fraudes por pirâmide, *cyber*-pornografia, apostas *online*) (LIGETI; VERVAELE; KLIP, 2018, p. 182-183).

Os riscos decorrentes dos cibercrimes podem ser variados, razão por que a adjetivação de um delito como sendo *cibernético* parece se dar menos pela identidade do bem jurídico a ser penalmente tutelado,[1] e mais pelo instrumento utilizado para o seu cometimento.

Por esse motivo, variadas são as condutas trazidas pela Convenção de Budapeste a serem criminalizadas pelos Estados-parte, desde as que surgiram na era digital até as já existentes, mas que passaram a utilizar a *internet* como meio de cometimento: acesso ilegal, interceptação ilícita, violação de dados, obstrução ou impedimento de acesso, uso indevido de aparelhagem, falsificação e fraude informática, pornografia infantil e violação de direitos autorais ou correlatos.

Buscou-se descrever condutas consideradas penalmente relevantes, eleitas como as mais sensíveis à época, para auxiliar o combate à criminalidade cibernética e evitar abusos decorrentes da legislação menos rigorosa de um Estado, que impactam outros países.

Antes da adesão do Brasil à Convenção, pelo transcurso do tempo, o legislador pátrio, seguindo a tendência internacional, já havia constatado a necessidade da criminalização de determinadas condutas mencionadas no texto convencional, como: o delito de invasão de dispositivo informático, previsto no art. 154-A, do Código Penal, acrescentado pela Lei 12.737/2012[2] e modificado pela Lei 14.155/2021 (art. 2º, da Convenção); o delito de pornografia infantil, previsto no art. 241 e seguintes, do Estatuto da Criança e do Adolescente, por meio da Lei 11.829/2008 (art. 9º, da Convenção); o delito de violação de direito autoral, previsto no art. 184, do Código Penal, por meio da Lei 10.695/2003 (art. 10, da Convenção). Nesses casos, a Convenção já tem aplicabilidade imediata, visto que existe um tipo penal equivalente em vigor, descrevendo a conduta considerada ofensiva a um bem jurídico, à qual é cominada uma pena.

Outros delitos informáticos (acesso não autorizado à rede, dispositivo ou sistema informatizado; obtenção, transferência ou fornecimento não autorizado de dados; divulgação ou utilização indevida de dados pessoais; dano informático; inserção ou difusão de vírus; entre outros) estavam inicialmente previstos no Projeto de Lei 84/1999, mas não se mantiveram na promulgação da Lei 12.735/2012. Há, ainda, outros projetos de lei que tramitam no Senado e na Câmara dos Deputados, especialmente o PL 5.441/2020, apensado ao PL 3.357/2015, que versam sobre delitos cibernéticos e contemplam os compromissos assumidos na Convenção.

Nessas hipóteses, ainda que a Convenção tenha *status* de lei federal e haja a compreensão, pelo Legislativo brasileiro, da relevância penal de tais condutas, a persecução penal resta obstada ante a garantia do princípio da legalidade estrita, que demanda complementação legal para que as medidas criadas sejam, de fato, aplicadas, seja pelo fechamento dos tipos penais com a descrição das condutas a serem incriminadas, seja pela determinação das possíveis penas a serem cominadas.

Deve haver cuidado com a tipificação de novas condutas trazidas pela Convenção, para não resultar em sobreposição com os tipos penais já previstos na legislação brasileira ou excesso punitivo. A análise do bem jurídico, a tipificação clara e a previsão de penas proporcionais são etapas fundamentais e que demandam discussão com certo nível de maturidade, para que não se torne mais uma norma penal ineficaz, a trazer insegurança jurídica e a permitir arbitrariedades no exercício do poder estatal.

3. Responsabilidade da pessoa jurídica por crimes cibernéticos

Além da preocupação de criar o *standard* de criminalização, a Convenção de Budapeste prevê, ainda dentro do capítulo de Direito Penal, outras formas de responsabilidade e sanções às pessoas jurídicas.

A Convenção de Budapeste prevê, em seu art. 12, a responsabilidade da pessoa jurídica pela prática dos crimes cibernéticos. Há discrepância na redação do artigo no idioma inglês da tradução adotada no Decreto 11.491/2023. No texto em inglês, usa-se apenas a expressão "*corporate liability*", sem adjetivar a responsabilidade como civil, penal ou administrativa,[3] e prossegue na redação determinando que os Estados-parte adotem medidas necessárias para assegurar que pessoas jurídicas possam ser responsabilizadas por crimes previstos na Convenção. Já no Decreto, utiliza-se o termo "responsabilidade penal da pessoa jurídica", assegurando que "pessoas jurídicas possam ser consideradas penalmente responsáveis".

A diferença na redação, embora pareça sutil, esclarece a aparente incompatibilidade do art. 12, partes 1 e 2, do Decreto, com a parte 3, que prevê que a responsabilidade da pessoa jurídica pode ser "civil, criminal ou administrativa". Ora, pelo Decreto, inicialmente a responsabilidade seria taxativamente penal e depois permitiria adequar aos princípios orientadores do Estado-parte. Contudo, o texto da Convenção, em realidade, permite que cada Estado decida, como for mais adequado ao seu ordenamento jurídico, a forma de responsabilização mais adequada e eficaz.

Além disso, a Convenção traz duas formas de responsabilização do ente coletivo: (i) "quando cometidos em seu benefício por qualquer pessoa física em posição de direção, que aja individualmente ou como integrante de um órgão da própria pessoa jurídica", com base no seu poder de representação, na autoridade para tomar decisões e de exercer o controle interno na pessoa jurídica; e (ii) quando outros indivíduos, despidos de tais características, praticarem crimes dentro do seu escopo de atuação, em benefício da pessoa jurídica, porque houve falha na supervisão ou o controle. Nesse segundo caso, orienta o Conselho da Europa que as medidas de controle esperadas sejam identificadas pelo tipo de negócio desenvolvido, pelo tamanho, pelo padrão de melhores práticas, o que significaria dizer que não é qualquer falha de vigilância que poderiam resultar numa responsabilização (COUNCIL OF EUROPE, 2021a).

Ainda, faz-se a ressalva de que a responsabilidade do ente coletivo deve ocorrer "sem prejuízo da responsabilidade criminal das pessoas naturais que tenham cometido o crime", e que as sanções a ela aplicadas, penais ou não, sejam "eficazes, proporcionais e dissuasivas".

O modelo proposto de responsabilidade da pessoa jurídica é bastante atrelado ao crime praticado pela pessoa física. Se compreendido como responsabilidade penal, como se fez constar no Decreto

11.491/2023, algumas considerações são necessárias a fim de analisar a sua compatibilidade com o ordenamento jurídico pátrio.

Em primeiro lugar, há previsão na Constituição de 1988 da responsabilidade penal da pessoa jurídica. O art. 173, § 5º, da CR, prevê a responsabilidade da pessoa jurídica, "sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular". Já no art. 225, § 3º: "As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados". Expressamente, o texto constitucional enumera bens jurídicos a possibilitar a responsabilização penal do ente coletivo. Como o que qualifica os delitos como cibernéticos não é o bem jurídico, é possível vislumbrar condutas que se enquadram nas hipóteses listadas, para essa forma de responsabilidade constante do decreto.

Em segundo lugar, o tema é, ainda, bastante controverso, seja pelo histórico que remonta ao brocardo *societas delinquere non potest*, seja pelas diversas dificuldades dogmáticas penais para que se conceba, efetivamente, um modelo de responsabilidade compatível com os princípios orientadores do Direito Penal brasileiro. Com o desenvolvimento teórico da responsabilidade penal das pessoas jurídicas, não se cogita mais um modelo de imputação por transferência ou de heterorresponsabilidade,[4] admitindo-se, em observância ao princípio da culpabilidade, tão somente um modelo de autorresponsabilidade.[5]

No caso da Convenção, atrela-se a responsabilidade do ente coletivo à prática de crimes pelos gestores ou diretores, mas faz a ressalva de que o indivíduo também deve ser punido. É uma responsabilidade do ente coletivo por ricochete, ou transferência, em que a conduta dolosa individual resulta na aplicação de uma pena à pessoa natural e ao ente coletivo, incorrendo em *bis in idem*. Na segunda hipótese, de responsabilidade por ausência ou deficiência do controle, estar-se-ia mais próxima de uma responsabilidade própria da pessoa jurídica, mas cuja teorização é ainda carente de refinamento dogmático para justificar a exigência do dever de controle por parte do ente coletivo.

Esses seriam pontos para o início de uma vasta discussão, com carência substancial sobre as teorias de responsabilidade penal da pessoa jurídica (sanções, dosimetria), e carência processual (rito).

4. A cooperação jurídica internacional para a obtenção de provas digitais

A Convenção de Budapeste traz relevantes novidades sobre cooperação jurídica internacional para obtenção de provas digitais (arts. 23 a 35), com o potencial de tornar mais eficiente a obtenção de provas entre o Brasil e outros 67 Estados.

Além de estimular os laços com outros Estados, a ratificação de um tratado com dispositivos de cooperação sobre provas digitais era há tempos devida, já que tais provas, pelas suas características específicas (volatilidade, ubiquidade e dispersão), diferem das provas corpóreas e requerem procedimentos cooperacionais específicos para a sua obtenção (BADARÓ, 2021).

Basta pensar que, atualmente, os dados digitais são acessíveis de forma remota de qualquer local (nuvem), ficando fisicamente armazenadas muitas vezes em um Estado diferente daquele em que está o usuário. Ademais, os dados em si são multiterritoriais ou aterritoriais, porque se movimentam com facilidade entre Estados, são divididos e replicados para locais diferentes e muitas vezes sequer se sabe onde estão (DASKAL, 2015, p. 365 *et seq.*; NOJEIM, 2018).[6]

Visando conferir a celeridade necessária à cooperação jurídica internacional probatória, a Convenção prevê dois instrumentos cautelares: quando há risco de perda ou modificação dos dados, o pedido de conservação de dados armazenados em computador, para um futuro pedido de acesso, busca e apreensão, guarda ou revelação (art. 29); e quando há necessidade de obtenção urgente de algum dado que auxilie a identificar a proveniência daquele dado, o pedido de revelação de dados específicos de tráfego para identificação do provedor de serviços e do caminho percorrido (art. 30).

A Convenção prevê também três instrumentos específicos para obtenção de provas digitais: pedido de busca, acesso, apreensão, guarda ou a revelação de dados armazenados por meio de computador (art. 31); pedido de interceptação de dados de tráfego em tempo real (art. 33); e pedido de interceptação ou gravação em tempo real do conteúdo de comunicações específicas transmitidas por meio de um sistema de computador (art. 34).

A Convenção traz, ainda, duas hipóteses para acesso transfronteiriço a dados armazenados em computador, sem a necessidade de cooperação jurídica internacional: quando houver consentimento daquele com autoridade legal para revelar os dados ou quando os dados estiverem em sistema de acesso público (art. 32).

Os potenciais riscos de excessos na utilização do dispositivo, dada a sua natureza unilateral, levaram o Comitê da Convenção a elaborar uma orientação interpretativa para o art. 32, sinalizando a sua aplicabilidade restrita aos casos em que se tem certeza de onde o dado esteja armazenado e o dever do Estado que acessa o dado de notificar o Estado em que o dado está localizado (COUNCIL OF EUROPE, 2014).

Para conferir a necessária eficiência dos instrumentos cooperacionais, foram trazidas alterações nos canais de transmissão dos pedidos. Apesar de a Convenção prever a intermediação pelas autoridades centrais, em caso de urgência, os pedidos podem ser enviados diretamente pelas autoridades judiciais do Estado requerente para suas congêneres no Estado requerido ou, não havendo, para a Interpol, desde que a autoridade central seja concomitantemente comunicada (art. 27). Ademais, foi criado o sistema de plantão 24 por 7, em que cada Estado indica um órgão de contato para, entre outros, receber comunicações urgentes de pedidos de prova digitais (art. 35).

Diferentemente de outros Estados que indicaram um único órgão para ambas as funções, o Brasil, no ato de sua ratificação, indicou o Departamento de Recuperação de Ativos e Cooperação Internacional como autoridade central e a Polícia Federal como órgão de enlace (COUNCIL OF EUROPE, 2006), demandando investimento na estrutura cooperacional do Ministério da Justiça.

A perspectiva trazida pelos novos instrumentos é positiva, mas deve ser acompanhada da regulamentação do rito cooperacional, de modo a permitir o acesso dos indivíduos afetados pelo ato cooperacional, a sua participação e controle, dentro de um marco de direitos e garantias.

Nesse ponto, menção honrosa merece o art. 15 da Convenção, que coloca, de forma explícita, a cooperação jurídica internacional dentro

do marco de direitos e garantias previstas em tratados internacionais de Direitos Humanos[7] e no princípio da proporcionalidade, prevendo inclusive a necessidade de controle judicial, fundamentação na aplicação e delimitação do alcance dos procedimentos cooperacionais.

5. Considerações finais

A Convenção de Budapeste foi incorporada no ordenamento jurídico brasileiro num momento em que diversos temas que tocam a criminalidade cibernética estão em voga, como o vazamento de dados, os golpes informáticos e o uso da *internet* para a disseminação das *fake news*.

A temática merece amplo debate, a fim de que o Estado alcance certo nível de maturidade para a criação de políticas públicas, incluindo-se uma política criminal adequada para o enfrentamento da questão, que certamente é muito mais ampla que a abordagem estritamente criminal.

No momento da seleção das condutas a serem criminalizadas trazidas na Convenção, porque o texto é datado, a adequação e a atualização das condutas à realidade de hoje é imprescindível. Também se faz necessária uma análise global do ordenamento jurídico pátrio, para que não haja excesso punitivo ou normas penais ineficazes, pois isso traria insegurança jurídica, a permitir arbitrariedades no exercício do poder estatal.

A tradução do decreto no que toca à responsabilidade penal da pessoa jurídica, que qualifica a responsabilidade do ente coletivo como penal, deve ser entendida como uma recomendação, e não um mandado. Até porque o nível de discussão para a criação de um modelo de imputação de responsabilidade penal do ente coletivo ainda parece incipiente no âmbito legislativo, demandando maior aprofundamento sobre a sua viabilidade, seja pelas hipóteses de responsabilização, seja pela adequação dos modelos de responsabilidade com os princípios orientadores do Direito Penal brasileiro.

Os novos instrumentos de cooperação jurídica internacional previstos na Convenção têm o potencial de agilizar e tornar mais eficiente a obtenção de provas. A sua efetividade depende, todavia, da adoção de medidas para regulamentar o rito cooperacional, permitindo a participação e o controle pelos indivíduos envolvidos e afetados pelos atos cooperacionais.

É o momento de olhar também para o futuro e iniciar um debate sobre a possibilidade de ratificação brasileira também do 2º Protocolo Adicional à Convenção (COUNCIL OF EUROPE, 2021b), aberto para adesão em 2022. Atualizado, o Protocolo prevê instrumentos específicos para cooperação direta entre autoridades do Estado requerente e o provedor de conteúdo no Estado requerido para a emissão de ordens de divulgação de nome de domínio e de informações cadastrais do assinante, regulamento para videoconferência e equipes conjuntas de investigação.

Notas

[1] Sobre o tema, Spencer Toth Sydow (2022, p. 164-180) defende existir um bem jurídico informático, que "possui parcela pública no que toca à sua segurança informática e à estabilidade de acesso à rede e aos serviços de utilidade pública — e a própria virtualidade o é — parcela privada no que toca à segurança informática em seu caráter privado de proteção aos elementos relativos a dados e sistemas de informação".

[2] É conhecida como "Lei Carolina Dieckmann", por suposto vazamento de fotos íntimas na *internet*, mas que atende à "demanda antiga do setor financeiro, duramente impactado com os golpes e fraudes eletrônicas, ainda que considerada uma lei absolutamente 'circunscrita', em comparação aos projetos sobre crimes cibernéticos que tramitavam no Congresso Nacional" (JESUS, MILAGRE, 2016, p. 85).

[3] Texto da Convenção em inglês disponível em: https://rm.coe.int/1680081561. Acesso em: 17 maio 2023.

[4] Nos modelos de heterorresponsabilização, responsabiliza-se a pessoa jurídica por atribuição, transferência, ricochete ou empréstimo dos atos praticados por uma pessoa natural que integra a empresa, atua no exercício de suas atividades e dentro de sua atribuição, como se fosse o órgão empresarial, em benefício da empresa, importando os seus elementos físicos e psicológicos (GALVÃO, 2020, p. 23).

[5] Os modelos de autorresponsabilidade penal da pessoa jurídica podem ser considerados uma "evolução gradativa" da heterorresponsabilidade, em que se busca uma responsabilização autônoma à individual, por fato próprio do ente coletivo, como não se organizar de modo a impedir ou dificultar a depuração da responsabilidade individual (SALVADOR NETTO, p. 102-103 e 119).

[6] Sobre o tema, antes da ratificação da Convenção de Budapeste, ver, entre outros, Ritzmann Torres (2022).

[7] Sobre uma visão contemporânea da cooperação internacional à luz dos direitos humanos, por todos, ver Carvalho Ramos (2023).

Referências

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, ano 29, n. 343, p. 7-9, jun. 2021. Disponível em: https://ibccrim.org.br/publicacoes/edicoes/747/8544. Acesso em: 30 maio 2023.

CARVALHO RAMOS, André de. *Curso de Direito Internacional Privado*. 3. ed. São Paulo: Saraiva, 2023.

COUNCIL OF EUROPE. *Convention on cybercrime*: Special edition dedicated to the drafters of the Convention (1997-2001). Estrasburgo: Council of Europe, 2021a. Disponível em: https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e. Acesso em: 14 maio 2023.

COUNCIL OF EUROPE. *Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. Estrasburgo: Council of Europe, 2021b. Disponível em: https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930. Acesso em: 14 maio 2023.

COUNCIL OF EUROPE. *T-CY Guidance Note # 3 Transborder access to data (Article 32) Adopted by the 12th Plenary of the T-CY (2-3 December 2014)*. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a. Acesso em: 30 maio 2023.

COUNCIL OF EUROPE. *Reservations and Declarations for Treaty No.185 – Convention on Cybercrime (ETS No. 185)*. 10 out. 2006. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0. Acesso em: 30 maio 2023.

DASKAL, Jennifer. The un-territoriality of data. *The Yale Law Journal*, v. 125, n. 2, p. 326-398, 2015. Disponível em: https://www.yalelawjournal.org/article/the-un-territoriality-of-data. Acesso em: 30 maio 2023.

GALVÃO, Fernando. *Teoria do crime da pessoa jurídica*: proposta de alteração do PSL nº 236/12. Belo Horizonte: D'Plácido, 2020.

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

LIGETI, Katalin; VERVAELE, John; KLIP, André. *Preventing and resolving conflicts of jurisdiction in EU Criminal Law*. Oxford: Oxford University Press, 2018, p. 182-183.

NOJEIM, Greg. Reforma do sistema MLAT entre privacidade e eficiência: os dilemas do acesso transnacional a dados de usuários. Tradução: Ana Luiza Araujo. *In*: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza (Orgs.). *Direitos fundamentais e processo penal na era digital*: Doutrina e prática em debate. Vol. I. São Paulo: InternetLab, 2018. pp. 176-200.

RITZMANN TORRES, Paula. Desafios contemporâneos do direito à prova: obtenção de dados digitais armazenados no exterior. *Revista da Faculdade de Direito da Universidade Federal de Uberlândia*, v. 50, n. 1, p. 229-252, 2022. https://doi.org/10.14393/RFADIR-50.1.2022.65264.229-252

SALVADOR NETTO, Alamiro Velludo. *Responsabilidade penal da pessoa jurídica*. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020.

SYDOW, Spencer Toth. *Curso de Direito Penal Informático*. 3. ed. Salvador: JusPodivm, 2022.

Autoras convidadas