XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

LITON LANES PILAU SOBRINHO

RIVA SOBRADO DE FREITAS

JÉSSICA FACHIN

I61

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Liton Lanes Pilau Sobrinho, Riva Sobrado De Freitas, Jéssica Fachin – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-65-5274-079-3
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 2. Dinâmicas da segurança pública e internacional. XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

O XXXI Encontro Nacional do CONPEDI ocorreu nos dias 27, 28 e 29 de novembo de 2024, em Brasília/DF. O evento teve como temática central "Um Olhas a partir da Inovação e das Novas Tecnologias".

As discussões realizadas durante o encontro, tanto nas diversas abordagens tecnológicas como nos Grupos de Trabalho (GTs), foram de grande relevância, considerando a atualidade e importância do tema.

Nesta publicação, os trabalhos apresentados como artigos no Grupo de Trabalho "Internet: Dinâmicas da Segurança Pública e Internacional I", no dia 29 de novembro de 2024, passaram por um processo de dupla avaliação cega realizada por doutores. A obra reúne os resultados de pesquisas desenvolvidas em diferentes Programas de Pós-Graduação em Direito, abordando uma parte significativa dos estudos produzidos no âmbito central do Grupo de Trabalho.

As temáticas abordadas refletem intensas e numerosas discussões que ocorrem em todo o Brasil. Elas indicam a urgência de pensar a tecnologia a partir dos direitos humanos, apontam para a problemática do discurso de ódio, indicando necessidade de educação para a cidadania digital, os desafios para a democracia frente à infodemia e ao contexto das fake news, bem como a definição desta e reflexões atuais e importantes sobre a regulação das plataformas digitais.

Esperamos que, por meio da leitura dos textos, o leitor possa participar dessas discussões e obter um entendimento mais amplo sobre o assunto. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e na organização do evento, cujas contribuições inestimáveis foram fundamentais, e desejamos uma leitura proveitosa!

Liton Lanes Pilau Sobrinho

(Universidade Federal de Santa Catarina)

Riva Sobrado de Freitas

(Universidade do Vale do Itajaí)

Danielle Jacon Ayres Pinto

(Universidade do Oeste de Santa Catarina)

Jéssica Fachin

(Universidade de Brasília e Faculdades Londrina)

A COOPERAÇÃO INTERNACIONAL EM PROCESSOS CRIMINAIS E AS NOVAS TECNOLOGIAS

INTERNATIONAL COOPERATION IN CRIMINAL PROCEEDINGS AND NEW TECHNOLOGIES

Werna Karenina Marques de Sousa [1]

Resumo

Nesta era digital, em que a informação viaja à velocidade da luz e as fronteiras são cada vez mais tênues, é crucial compreender as consequências, os desafios e as oportunidades que a tecnologia traz ao domínio da aplicação da lei internacional. analisar as consequências destas novas tecnologias. Um dos resultados mais significativos é a globalização do crime. Atualmente, as organizações criminosas operam facilmente através das fronteiras, utilizando ferramentas digitais para orquestrar esquemas complexos, desde ciberataques ao tráfico de droga. Esta globalização exige uma resposta internacional proporcional. Para tanto, esta pesquisa adota uma abordagem qualitativa para investigar a como os mecanismos tecnológicos têm ajudado e seus impactos na cooperação internacional em processos criminais, combinando revisão bibliográfica e estudo de casos práticos. A integração de teoria e prática visa analisar criticamente como a gestão de dados processuais pode apoiar decisões estratégicas na área da cooperação internacional em processos criminais, evitando a impunidade de seus autores.

Palavras-chave: Novas tecnologias, Cooperação internacional, Inteligência artificial, Processo criminal, Soberania digital

Abstract/Resumen/Résumé

In this digital era, where information travels at the speed of light and borders are increasingly porous, it is crucial to understand the consequences, challenges, and opportunities that technology brings to the domain of international law enforcement. One of the most significant outcomes is the globalization of crime. Nowadays, criminal organizations easily operate across borders, using digital tools to orchestrate complex schemes, from cyberattacks to drug trafficking. This globalization demands a proportional international response. To this end, this research adopts a qualitative approach to investigate how technological mechanisms have aided and their impacts on international cooperation in criminal proceedings, combining a literature review and practical case studies. The integration of theory and practice aims to critically analyze how the management of procedural data can support strategic decisions in the field of international cooperation in criminal proceedings, preventing the impunity of the perpetrators

---

[1] Professora Adjunta de Direito no Departamento de Direito- DIR/UFRN. Doutora em Direito com duplo diploma na Universite Grenoble-Alpes France e na Universidade Federal da Paraiba – UFPB.

Keywords/Palabras-claves/Mots-clés: New technologies, Digital sovereignty, Criminal procedure, International cooperation, Artificial intelligence

1. INTRODUÇÃO

A história do crime informático remonta à década de 1960, quando os primeiros artigos trataram de manipulação de computadores, sabotagem de computadores, uso ilegal de sistemas computacionais e espionagem informática.

Nos anos 1980 e 1990, o crime informático deixou de se limitar ao crime econômico, passando a incluir ataques contra uma gama diversificada de interesses, como violações de privacidade e de direitos autorais, além do uso de computadores e sistemas de comunicação pelo crime organizado.

O advento da Internet trouxe mudanças substanciais: no nível fenomenológico, houve a disseminação de conteúdos ilegais (infrações de propriedade intelectual, pornografia infantil, incitação ao racismo e à xenofobia, etc.), acesso ilegal a sistemas computacionais, interferência em sistemas e dados, interceptação ilegal de transmissões não públicas de dados computacionais, além de novas ferramentas de comunicação também úteis para a preparação de crimes graves, como o terrorismo.

A proliferação mundial das tecnologias da informação e comunicação facilitou a prática e a preparação desses tipos de atividades criminosas, que representam ameaças não apenas à confidencialidade, integridade ou disponibilidade de sistemas e dados computacionais e à segurança de infraestruturas críticas, mas também aos direitos de propriedade intelectual, à propriedade e à confiança pública.

Duas questões precisam ser levantadas: é possível prevenir a repetição de delitos? deve-se prevenir essa repetição por meio dessas ferramentas previsionais? A questão da possibilidade de prevenir a repetição de delitos através da inteligência artificial é, portanto, levantada, assim como a pertinência do uso dessas ferramentas no sistema penal.

O estudo tem como objetivo analisar o impacto das novas tecnologias frente à cooperação internacional em processos penais. A análise avançada de dados e a inteligência artificial podem ajudar a prever e prevenir crimes. Os algoritmos de policiamento preditivo têm sido utilizados em várias cidades a nível mundial para afetar recursos de forma mais eficiente e reduzir as taxas de criminalidade.

A tecnologia *Blockchain* pode aumentar a transparência e a segurança das transações financeiras internacionais, dificultando o branqueamento de capitais por parte dos criminosos.

A cooperação entre bancos internacionais e agências de aplicação da lei para acompanhar e rastrear fluxos financeiros ilícitos utilizando a tecnologia *blockchain*.

A realidade virtual pode revolucionar a forma como as provas são apresentadas na instrução processual, permitindo reconstituições mais imersivas e exatas de cenas de crime. A utilização da RV no Tribunal Penal Internacional para apresentar provas em casos complexos que envolvem crimes de guerra e atrocidades.

As novas tecnologias continuarão a remodelar o panorama da cooperação internacional em processos penais. As consequências são profundas, os desafios são complexos, mas as oportunidades são vastas. Para combater eficazmente a criminalidade mundial e defender a justiça, temos de adaptar os nossos sistemas jurídicos, fomentar a confiança internacional e tirar proveito do poder da tecnologia. A colaboração internacional, alicerçada num compromisso partilhado com o Estado de Direito e os Direitos humanos, continua a ser a chave para resolver estas questões prementes.

Para a condução desta pesquisa, optou-se pelo método dedutivo, conforme descrito por Mezzaroba e Monteiro (2009). Nesse sentido, considerou-se a aplicação rigorosa dos princípios da lógica, partindo-se de argumentos gerais para argumentos específicos. Essa abordagem garante uma relação direta entre as conclusões formais enunciadas e as premissas previamente estabelecidas. Adicionalmente, foram realizados estudos bibliográficos e normativos relacionados ao objeto de estudo.

2. A EVOLUÇÃO DOS ACORDOS E TRATADOS INTERNACIONAIS PODE FACILITAR A COOPERAÇÃO

O instrumento internacional mais relevante que estabelece diretrizes para leis e procedimentos no enfrentamento ao crime na internet em nível global tem sido a Convenção sobre Cibercrime, também conhecida como Convenção de Budapeste. Em 23 de novembro de 2001, 25 dos 47 Estados Membros do Conselho da Europa e quatro países não membros assinaram a Convenção sobre Cibercrime. Na celebração de 20 anos da convenção, em 17 de novembro de 2021, foi publicado um 2º Protocolo Adicional. Essa convenção foi ratificada por 66 Estados, incluindo todos os Estados europeus (exceto a Irlanda); 20 Estados basearam sua legislação na Convenção, enquanto quase 50 se inspiraram nela. Isso mostra que o texto tem um alcance que vai além da jurisdição do Conselho da Europa.

A harmonização das medidas processuais (Capítulo II) e da assistência mútua internacional (Capítulo III) resulta na troca de dados pessoais (dados de tráfego, conteúdo das comunicações e outros tipos de informações). A necessidade de encontrar o equilíbrio correto entre segurança e direitos fundamentais é crucial para a eficácia e a confiança na Convenção.

A Convenção de Budapeste não se aplica apenas ao cibercrime, pois aborda, de maneira geral, a implementação de procedimentos e mecanismos relacionados a diversas atividades de investigação criminal, como: inspeções, buscas, apreensão de correspondência e outros itens, custódia, inquéritos urgentes, etc relacionados a outros tipos de crimes – ou seja, delitos "convencionais" – sempre que as provas a serem coletadas estejam ou possam ser encontradas em mídia eletrônica e/ou com a ajuda de meios eletrônicos, conforme artigos 14 e 19 da Convenção:

> Artigo 14 - Âmbito de aplicação dos dispositivos processuais
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer os poderes e procedimentos previstos nesta seção para o fim específico de promover investigações ou processos criminais.
> [...]
> Artigo 19 - Busca e apreensão de dados de computador
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para busca ou investigação, em seu território:
> a. de qualquer sistema de computador ou de parte dele e dos dados nele armazenados; e
> b. de qualquer meio de armazenamento de dados de computador no qual possam estar armazenados os dados procurados em seu território. (Brasil, 2023)

A Convenção prevê diversos mecanismos de cooperação e assistência mútua entre os países signatários, também para fins de extradição. Eles se aplicam não apenas às infrações penais relacionadas a sistemas e dados informáticos, mas também à coleta de provas em formato eletrônico de qualquer infração penal. Isso pode envolver um número considerável de casos, uma vez que as infrações em questão são punidas com a privação de liberdade por um período máximo de pelo menos um ano, como dispõe os artigos 23 e 24:

> Artigo 23 - Princípios gerais da cooperação internacional
> As Partes cooperarão entre si, de acordo com as disposições deste capítulo, e por meio da aplicação de instrumentos internacionais pertinentes de cooperação internacional em assuntos penais, de ajustes firmados com base em legislação uniforme ou de reciprocidade, e da legislação doméstica, o mais possível, para a realização das investigações ou procedimentos acerca de crimes de computador, ou para a coleta de provas eletrônicas desses crimes.
> Artigo 24 - Extradição
> 1.a. Este Artigo aplica-se à extradição entre Estados a respeito dos crimes tipificados de acordo com os Artigos de 2 a 11 desta Convenção, desde que tais infrações sejam puníveis de acordo com as leis penais das duas Partes com

> pena privativa de liberdade cujo período máximo de seja de pelo menos 1 (um) ano, ou por uma sanção mais severa.
> b. Quando uma pena mínima diferente for prevista em conformidade com um acordo de legislação uniforme ou de reciprocidade, ou conforme um tratado de extradição, inclusive a Convenção Europeia sobre Extradição (ETS n. 24), e quando esses pactos sejam aplicáveis a duas ou mais Partes, deverá prevalecer a pena mínima estabelecida de acordo com esses ajustes ou tratados. (Brasil, 2023)

Dado esse contexto, as investigações criminais realizadas nos países, incluindo as investigações decorrentes de pedidos de cooperação internacional sob a Convenção, podem, em última análise, resultar na coleta e troca de uma quantidade considerável de dados pessoais (incluindo dados de tráfego telefônico e de internet) que podem não estar diretamente relacionados ao cibercrime, ou que podem estar relacionados a atividades totalmente lícitas.

Portanto, as medidas em questão produzem efeitos especialmente significativos sobre os direitos e liberdades dos titulares de dados. Antes do início do processo de ratificação, houve casos significativos na Itália em que, por exemplo, foram realizadas buscas em redações de jornais e/ou nas residências de jornalistas, em cumprimento a ordens emitidas por autoridades judiciais.

O texto final da Convenção levou em consideração apenas parcialmente as objeções e sugestões apresentadas pelas Autoridades de Proteção de Dados (DPAs) europeias. Uma emenda importante que foi feita para acomodar parcialmente as preocupações do referido órgão, diz respeito à inclusão de disposições mais específicas quanto aos critérios que justificam a adoção das medidas previstas na Convenção, em termos de necessidade, adequação e proporcionalidade, conforme exigido pelos instrumentos de proteção de dados mencionados anteriormente.

> Os redatores da Convenção de Budapeste debateram aspectos importantes como o direito material, processual e a competência. Diante disso, tal convenção foi elaborada não somente para criar novos tipos penais, mas também para estipular normas de processo penal, conciliando procedimentos de direito penal internacional e estabelecendo acordos referentes à tecnologia da informação (Boiteux, 2004, p. 170, *apud*, Cidrão, Muniz, Alves, 2018, p. 78).

Em particular, o Artigo 15 da Convenção exige que as partes signatárias garantam que a prestação de assistência esteja sujeita às condições e salvaguardas previstas em suas legislações nacionais. As medidas de assistência em questão devem prever a proteção adequada dos direitos humanos fundamentais, em especial aqueles estabelecidos na Convenção Europeia

dos Direitos Humanos, cujo Artigo 8 se refere ao direito à privacidade. Além disso, devem assegurar a conformidade com o princípio da proporcionalidade.

> Artigo 15 - Condições e garantias
> 1. Cada Parte assegurará que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos nesta seção sujeitem-se às condições e garantias instituídas na sua legislação interna, que estabelecerá proteção adequada aos direitos humanos e às liberdades públicas, incluindo os direitos nascidos em conformidade com as obrigações que esse Estado tenha assumido na Convenção do Conselho da Europa para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, de 1950, na Convenção Internacional da ONU sobre Direitos Civis e Políticos, de 1966, e em outros instrumentos internacionais de direitos humanos, e que tais poderes e procedimentos incorporarão o princípio da proporcionalidade.
> 2. Tais condições e garantias incluirão, quando seja apropriado, tendo em vista a natureza do poder ou do procedimento, entre outros, controle judicial ou supervisão independente, fundamentação da aplicação, e limitação do âmbito de aplicação e da duração de tais poderes ou procedimentos.
> 3. Desde que conforme ao interesse público, em especial a boa administração da justiça, cada Parte levará em conta o impacto dos poderes e procedimentos previstos nesta seção sobre os direitos, obrigações e legítimos interesses de terceiros. (Brasil, 2023)

A aplicação do princípio da proporcionalidade é estabelecida pela Convenção como um requisito obrigatório para a aplicação adequada da própria Convenção. Portanto, é necessário que este princípio seja incluído, caso ainda não esteja, e desenvolvido de maneira apropriada na legislação nacional dos países que cooperam. Para isso, cada uma das legislações relevantes que regulam as investigações e os trabalhos preparatórios relacionados aos processos criminais deve conter uma disposição *ad hoc*, segundo a qual as atividades investigativas e processuais devem ser conduzidas pelas autoridades judiciais e/ou policiais de acordo com uma abordagem proporcional e seletiva, ou seja, levando em consideração os dados e informações que são relevantes e não excessivos em relação às investigações em andamento, e aplicando mecanismos igualmente proporcionais. (Cidrão, Muniz, Alves, 2018)

Alternativamente, pode-se imaginar uma única regra geral a ser incluída no ato de ratificação da Convenção e, posteriormente, incorporada à legislação processual penal. As cláusulas de proporcionalidade em questão também devem se aplicar a outras atividades investigativas mencionadas na Convenção, independentemente de já estarem regulamentadas pela legislação nacional.

De acordo com o Artigo 22 da Convenção, as partes signatárias devem adotar as medidas necessárias para estabelecer jurisdição sobre qualquer infração prevista na Convenção, inclusive nos casos em que a infração tenha sido cometida fora do território nacional. Para oferecer as mais amplas salvaguardas possíveis aos cidadãos, é necessário estabelecer critérios

apropriados que facilitem a perseguição de crimes informáticos por um Estado sempre que uma determinada infração puder ser considerada como tendo sido cometida "no exterior" sob a legislação vigente – o que, atualmente, é frequentemente o caso.

> Artigo 22 - Jurisdição
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer jurisdição sobre qualquer dos crimes tipificados de acordo com os Artigos de 2 a 11 desta Convenção, quando a infração for cometida:
> a. no seu território; ou
> b. a bordo de uma embarcação de bandeira dessa Parte; ou
> c. a bordo de uma aeronave registrada conforme as leis dessa Parte; ou
> d. por um seu nacional, se o crime for punível segundo as leis penais do local do fato ou se o crime for cometido fora da jurisdição de qualquer Parte. (Brasil, 2023)

Sempre existe um questionamento se as convenções regionais podem exercer autoridade. Diversos acordos incluem disposições relativas ao espaço digital, seja como foco principal, seja como parte dos temas que abordam. Em ordem cronológica, pode-se citar: a Organização de Cooperação de Xangai (OCX, 2001), a Convenção de Budapeste do Conselho da Europa sobre Cibercriminalidade (2001), a Convenção da Commonwealth (2002), a Convenção dos Países Árabes do Cairo (2010) e a Convenção de Malabo dos países da União Africana (2014). Em relação à primeira, não é surpreendente que ela não possa servir de modelo, uma vez que entre seus membros estão a Rússia, a China e o Paquistão, e entre os observadores, o Afeganistão, a Bielorrússia e o Irã como dialogar sobre autoridade com Estados que negam os princípios democráticos? Os acordos da *commonwealth* e do Cairo parecem não ser determinantes, dada sua fraca ou inexistente implementação. (Watin-Augouard, 2022)

Os Estados africanos começam a ratificar um texto que, assim, ganha mais peso, a Convenção de Budapeste é vinculativa, ela tem efeito direto sobre as regras de direito penal e de procedimento penal dos Estados signatários, permitindo que cada Estado exerça sua autoridade respeitando a soberania dos outros, ao mesmo tempo que torna mais eficaz a luta contra a cibercriminalidade. Apesar dessa força, a Convenção não foi ratificada pela Rússia, China, Cuba, Irã, etc., ou seja, não produz nenhum efeito nos Estados de onde provêm muitos dos ciberataques. A União Europeia pode oferecer uma resposta mais abrangente, limitada em termos de espaço, mas com uma influência que ultrapassa suas fronteiras?

O Brasil é signatário de várias convenções internacionais, e novos acordos podem agilizar as investigações transfronteiriças. A participação do Brasil na Convenção de Budapeste sobre Crimes Cibernéticos permitiu uma troca de informações mais fácil nas investigações de crimes cibernéticos, contribuindo para o combate às atividades criminosas em linha.

Enquanto o Brasil e o mundo lidam com as consequências, desafios e oportunidades apresentados pelas novas tecnologias na cooperação internacional em processos criminais, fica claro que a colaboração é fundamental. A globalização do crime necessita de uma estrutura legal harmonizada e de maiores capacidades forenses digitais. Embora existam desafios, o potencial para uma melhor cooperação e a resolução bem-sucedida de crimes transnacionais está ao nosso alcance.

3. INVESTIGAÇÃO FORENSE DIGITAL

A investigação digital é um estudo computacional que utiliza diferentes operações de detecção, preservação e recuperação de provas digitais presentes em um dispositivo informático, baseando-se em conhecimentos sobre hardware e software. O *streaming* de vídeo permite aos usuários acessar conteúdos variados de áudio e vídeo. Aqui, ele é objeto de análises forenses com o objetivo de determinar os tipos de evidências digitais que podem ser extraídas dos dispositivos informáticos. No caso em que os cookies e o histórico sejam apagados pelo usuário, é possível reconstituí-los a partir da memória RAM. (Ange, 2016)

As atividades no navegador preservam informações valiosas que ajudam a rastrear os vídeos acessados pelo usuário. As principais informações, chamadas de trilhas externas, são as seguintes: o histórico de navegação, os cookies e o cache de memória. O arquivo de histórico pode ser apagado pelo usuário, mas é possível recuperá-lo realizando uma restauração do sistema para um ponto de restauração anterior à data presumida da ação. A recuperação do estado do sistema para uma data anterior permite analisar o histórico como se ele nunca tivesse sido apagado pelo navegador. (Ange, 2016)

Algumas ferramentas de software oferecem maior precisão no histórico de navegação, elas permitem observar todas as conexões de um usuário no navegador, seu nome de perfil, a hora exata da visita ao site, bem como o número de visitas à página consultada. Também é possível realizar uma triagem com base na data, no nome da página e no navegador e, também, revela claramente o nome do vídeo assistido.

A investigação digital com o objetivo de comprovar a visualização de um vídeo no *site* exige uma abordagem precisa e rigorosa. Primeiramente, a investigação digital de vídeos e os princípios de funcionamento, em seguida é necessário definir um procedimento de investigação em um ambiente restrito: esse procedimento consiste em analisar as trocas de pacotes de rede, os processos executados, as memórias relacionadas às atividades do navegador e a memória volátil do usuário. Dessa análise, conclui-se que a maioria das trilhas

da atividade de *streaming* está contida na memória *cache* reservada às atividades do navegador. (Ange, 2016)

A análise do histórico e da memória alocada ao navegador permite identificar a URL do vídeo em questão, o horário da atividade e o nome do perfil do usuário. De acordo com Ange (2019), um estudo mais aprofundado sobre a memória poderia possibilitar a reconstituição completa do vídeo. A restauração do vídeo a partir da memória constituiria uma prova irrefutável do uso do *streaming* de vídeo e representaria um grande avanço para o campo da investigação digital de vídeos.

No mesmo sentindo, o reconhecimento facial é uma ferramenta relevante utilizada pela investigação forense digital, observa-se o exemplo a seguir:

> Um exemplo do uso dessas ferramentas ocorreu durante as investigações sobre a invasão do Capitólio nos Estados Unidos (janeiro, 2021). Incentivados por um discurso do ex-presidente Donald Trump, milhares de seus apoiadores invadiram o prédio do governo e entraram em confronto com a polícia. Além de ser noticiado pela mídia tradicional, o ato foi documentado por meio de imagens e vídeos compartilhados ao vivo pelos próprios invasores. Apesar de os vídeos capturarem os invasores à medida que adentravam as salas do Capitólio, seria necessário um esforço considerável para recuperar suas identidades. Dessa forma, investigadores utilizaram algoritmos de reconhecimento facial para identificar possíveis suspeitos, associando os vídeos produzidos com fotos disponíveis na internet. (Padilha, 2021)

Novas tecnologias oferecem oportunidades para uma perícia digital mais eficiente, auxiliando nas investigações criminais. O Brasil tem feito progressos nessa área, aumentando sua capacidade de analisar evidências digitais. As agências de aplicação da lei brasileiras têm agora unidades especializadas equipadas com tecnologia de ponta. Isto melhorou a sua capacidade de investigar casos que envolvem fraudes em linha, pirataria informática e ciberataques e a buscar por indivíduos com mandado de prisão expedidos e que se encontram em locais desconhecidos.

4. SOBERANIA DIGITAL

O espaço digital é erroneamente denominado assim, devido às fontes utópicas que influenciaram sua criação e desenvolvimento. A Declaração de Independência do Ciberespaço, pronunciada em 1996 por John Perry Barlow, sem dúvida promoveu a ideia de que o espaço digital era um espaço "à parte", podendo ser distinto dos espaços físicos (terra, mar, ar) e escapar das regras que os regem, organizando as atividades humanas que nele ocorrem. Na realidade, o espaço digital é um substrato que irriga, permeia todos os espaços nos quais

vivemos. Ele é "tudo para todos, em todo lugar, para tudo, em tudo" e deve acelerar sua penetração com o desenvolvimento de tecnologias disruptivas, especialmente com o avanço da 5G, da inteligência artificial e da computação quântica. (Watin-Augouard, 2022)

A hiperconexão refuta os cientistas do Vale do Silício que sonhavam com um espaço livre de qualquer restrição, de qualquer regulação. Mas como compreender a autoridade no espaço digital? No mundo real, a autoridade é indissociável do Estado de Direito, ela é codificada em seus fundamentos, em sua materialidade, confere o direito de comandar, de obter obediência, de sancionar que se exerce na verticalidade. No espaço digital, os paradigmas são desafiados: a autoridade tradicional deve se adaptar, se inserir em um sistema em rede, por construção descentralizada. O fim da utopia marca nosso tempo, pois não se pode estar em outro lugar em um substrato que agora penetra nossos próprios corpos.

No mesmo sentido, Francisco Balaguer Callejón (2023, p.2) afirma:

> Os grandes agentes globais, os especuladores financeiros e as companhias tecnológicas liberaram forças que o Estado não pode controlar e diante das quais a constituição se encontra impotente. A crise sanitária e tudo o que lhe seguiu não fizeram mais que agravar a situação, consolidando tendências que tinham se manifestado já nos dois primeiros, decênios do novo século. A constituição regula um mundo que em parte já não existe ou é socialmente irrelevante, se levarmos em consideração as novas gerações de nativos digitais.

A transformação digital desafia os fundamentos tradicionais do Estado, sob os impactos das multinacionais que pretendem o monopólio mundial. No entanto, os Estados se apropriam da internet, pelo menos porque lhes é exigido que exerçam autoridade para criar uma ordem pública que proteja as pessoas físicas e jurídicas, e porque buscam uma soberania, uma autonomia estratégica. Mas eles não podem, sozinhos, atingir esse objetivo e devem inserir sua intervenção em uma governança "multissetorial".

No entanto, o Estado deve recuperar sua autoridade, nem que seja para garantir a segurança de pessoas e bens diante dos predadores. O retorno do Estado passa por uma cooperação internacional, sem a qual não é possível implementar uma governança do espaço digital. O substrato digital desafia a noção de Estado, tal como foi definida por Carré de Malberg (1921, *apud*, Watin-Augouard, 2022) "Comunidade de homens, fixada em um território próprio e possuindo uma organização da qual resulta, para o grupo considerado em suas relações com seus membros, um poder supremo de ação, de comando e de coerção.".

A internet desafia a soberania com sua malha (quase) sem fronteiras, exceto para os Estados que buscam um controle do ciberespaço. O poder de emitir moeda é contrariado pelos criptoativos que, na esteira do *Bitcoin*, buscam competir com as moedas oficiais. O poder de

criar leis é contestado, ou até mesmo afastado, pelas normas de origem externa, principalmente anglo-saxônicas, que são impostas na falta de terem sido inspiradas. O exemplo das cláusulas gerais de uso, que estão inscritas nos contratos de serviço dos GAFAM (Google, Apple, Facebook, Amazon e Microsoft), é particularmente explícito, na medida em que fazem autoridade na relação com o cliente, mesmo sendo contrárias ao direito interno. (Watin-Augouard, 2022)

O código é a lei, segundo Lawrence Lessig (2000), destacando assim a autoridade do algoritmo, que se substitui às formas clássicas de autoridade para dizer o que se deve ou não fazer, aceitar ou recusar: Esse regulador é o código, o software e o hardware que fazem do ciberespaço o que ele é. Esse código, ou essa arquitetura, define a maneira como se vive o ciberespaço, determina se é fácil ou não proteger a privacidade ou censurar a palavra, também, determina se o acesso à informação é global ou setorizado e tem impacto sobre quem pode ver o quê, ou sobre o que é monitorado. Quando se começa a entender a natureza desse código, percebe-se que, de várias maneiras, o código do ciberespaço regula.

Os países estão cada vez mais a afirmar a sua soberania digital, o que leva a políticas de localização de dados e a restrições à partilha internacional de dados. O Brasil tem contemplado tais políticas, o que poderia dificultar as investigações criminais internacionais. A proposta do Brasil de implementar requisitos de localização de dados suscitou preocupações entre os investigadores internacionais. Tal poderia limitar o intercâmbio de provas cruciais em casos transnacionais.

A União Europeia pode afirmar sua autoridade em um mundo bipolar marcado pelo antagonismo China/EUA? É importante notar que a UE inicialmente considerou o espaço digital através do Mercado Comum, que se tornou o Mercado Único. A defesa do consumidor é o fio condutor que se manifesta por meio de seus regulamentos e diretivas.

5. USO DA INTELIGÊNCIA ARTIFICIAL EM CASOS CONCRETOS

Ao integrar tecnologias como Machine Learning e Big Data, a IA pode identificar padrões comportamentais, antecipar tendências criminais e otimizar o direcionamento de recursos policiais. Além disso, a utilização ética e transparente da IA pode contribuir para uma abordagem mais equitativa no combate ao crime, respeitando os direitos individuais e promovendo uma segurança pública mais eficiente e responsiva. (Oliveira, Ávila, 2019)

A questão deste artigo, centra-se na eficácia e nos desafios do uso da inteligência artificial (IA) no combate ao crime no Brasil. Busca-se investigar em que medida as tecnologias

de IA, como Machine Learning, Big Data e Redes Neurais Artificiais, têm impacto na prevenção e na resposta aos crimes, considerando a complexidade do cenário mundial.

O uso da inteligência artificial como uma ferramenta para a instituição judicial gerenciar a criminalidade pode parecer irrealista, mas a realidade é bem diferente, pois o movimento de automação da justiça penal está em andamento. Algoritmos capazes de antecipar o comportamento humano e avaliar a periculosidade dos indivíduos poderiam, um dia, ser explorados pelas autoridades judiciais, não para prevenir a prática de um delito (esse é o papel reivindicado pela polícia preditiva com ferramentas como o Predpol), mas para ajudá-las a tomar decisões sobre liberação durante a custódia ou para uma libertação condicional ou escolher a pena mais adequada. No futuro próximo, um certo número de decisões poderia, portanto, ser tomadas graças a ferramentas de antecipação de risco ou chamadas previsionais. (Oliveira Junior, Santos, 2022)

As ferramentas previsionais apresentam uma série de vantagens para a justiça penal. Elas podem apoiar a instituição judicial, mais especificamente, os tomadores de decisão, ou seja, os magistrados da esfera repressiva. Não seria esta uma ajuda inestimável para o juiz, que encontraria nessas ferramentas respostas para questões cruciais como: deve-se condenar o indivíduo a uma pena de prisão? O condenado cometerá novos delitos se for liberado antecipadamente? Diante dessas questões cotidianas, muitos magistrados poderiam ser aliviados na tomada de decisão. Além disso, essas tecnologias poderiam contribuir para fortalecer a segurança jurídica em benefício dos jurisdicionados (vítimas e acusados), já que a decisão não seria mais tomada por um magistrado, mas por uma ferramenta que analisou, de maneira científica, constantes e variáveis objetivas e externas. (Oliveira Junior, Santos, 2022)

Por fim, as ferramentas previsionais permitiriam aumentar a eficácia da repressão penal, evitando a liberação de indivíduos perigosos, reforçando, assim, a proteção da sociedade. Estes são alguns exemplos das contribuições da inteligência artificial para o sistema judicial. Conscientes desses potenciais benefícios, os políticos desejam utilizar essas ferramentas previsionais no serviço da justiça penal.

No entanto, essas técnicas também representam um perigo potencial para os direitos e liberdades fundamentais, devido a resultados que podem ser errôneos ou discriminatórios. Além disso, substituir o juiz por uma máquina poderia limitar o direito de acesso a um tribunal independente e imparcial, além de restringir a individualização da pena. Apesar dessas desvantagens, o futuro das ferramentas previsionais nos sistemas judiciais parece ser traçado pelo legislativo, impulsionados pelos desenvolvedores dessas tecnologias. Assim, a justiça poderia, no futuro, tornar-se algorítmica, automatizada ou simulada. (Moleirinho, 2021)

Em matéria penal, essa tecnologia poderia ser usada para prevenir o risco penal em um sentido amplo, seja para avaliar o risco de reincidência ou repetição de um delito por um suspeito ou condenado. Em outras palavras, as ferramentas previsionais seriam um novo indicador, permitindo limitar o perigo de repetição de infrações penais. Essa utopia, sempre buscada nas sociedades, seria alcançável por meio da inteligência artificial? Por enquanto, o uso desses algoritmos pelas autoridades policiais durante uma investigação ou pelo juiz no contexto de um processo penal ainda está em estágio embrionário. (Moleirinho, 2021)

A busca pela prevenção do risco penal e pela avaliação da periculosidade suscita o temor do ressurgimento de pensamentos deterministas, baseados na ausência de livre-arbítrio dos indivíduos. De fato, seria fácil admitir a ideia de que certos indivíduos são predeterminados a cometer infrações, o que justificaria uma pena rigorosa acompanhada de medidas de segurança. Esse determinismo latente ocorreria em detrimento do princípio da individualização da pena amplamente aceito desde 1945 na maioria dos sistemas judiciais ocidentais. (Castrillón, Córdoba, Castaño, 2008)

Na França, foi a doutrina da nova defesa social desenvolvida por Marc Ancel que lançou as bases do direito penitenciário moderno. A abordagem determinista e punitiva foi assim substituída por um sistema voltado para a readaptação social do indivíduo que pratica o fato criminoso. A ideia original consiste em afirmar que, ao (re)adaptar o indivíduo, o qual possui livre-arbítrio, as condições para a delinquência desaparecerão, permitindo, ao final, prevenir de forma duradoura a prática de infrações. No entanto, se algoritmos previsionais forem desenvolvidos, as garantias necessárias devem ser instauradas para evitar que sejam explorados sob uma perspectiva determinista e que os usuários (magistrados) não ignorem o objetivo de reinserção (Nicolas-Gréciano, 2021).

Além disso, em virtude do princípio da individualização da pena, o juiz deve basear-se em elementos objetivos (formação, emprego, acompanhamento médico-social regular, etc.) para encontrar a pena mais adequada ao condenado. Esse princípio, de valor constitucional, deve, igualmente, ser respeitado pelos instrumentos previsionais. Consequentemente, o uso de algoritmos de previsão do risco penal não deve alterar nem desconsiderar os objetivos de individualização e de reinserção da pena. (Nicolas-Gréciano, 2021).

Para conciliar as vantagens da inteligência artificial com as exigências do processo justo e da individualização das penas, os softwares de análise do risco penal devem ser considerados como instrumentos de apoio à tomada de decisão policial e judicial. As informações obtidas por meio dessas ferramentas devem necessariamente ser contextualizadas com os outros elementos reunidos pela instituição judiciária. Em suma, o resultado da avaliação do risco penal é uma

informação entre outras (perícia psicológica, antecedentes criminais, contexto familiar, social e econômico), e a decisão não pode basear-se exclusivamente nele.

Da mesma forma, não pode haver uma hierarquia preestabelecida entre a predição e os demais elementos à disposição do juiz, pois, se uma superioridade fosse conferida aos instrumentos previsionais, dada a possibilidade de erros, ocorreriam inevitavelmente violações às liberdades fundamentais. Para que essa garantia de ausência de hierarquização entre as informações obtidas seja eficaz, ela deve estar prevista em lei e não admitir nenhuma exceção.

Partindo de uma constatação ambígua, parece necessário considerar uma outra utilização da inteligência artificial no âmbito penal. Assim, não é a posição, mas a própria função desses instrumentos que deveria ser repensada. Em vez de utilizar a inteligência artificial como uma ferramenta preventiva, determinista e punitiva, os algoritmos poderiam ser desenvolvidos para servir à individualização da pena. Reunindo elementos objetivos de personalidade (formação, emprego, acompanhamento médico-social regular), bem como as informações detidas pelas instituições e organismos públicos, a inteligência artificial poderia centralizar grandes quantidades de dados de caráter econômico, social e sanitário e processá-los em tempo recorde (Nicolas-Gréciano, 2021).

Na era dos dados abertos (*open data*) das decisões judiciais e com base no funcionamento da análise de megadados (*big data analytics*), as conclusões tiradas dessas numerosas informações brutas poderiam ser comunicadas rapidamente ao juiz, que, em muitos casos, deve tomar decisões em prazos muito curtos, especialmente no âmbito de procedimentos acelerados.

O juiz teria então os meios para proferir a pena mais adequada à situação do indivíduo e aos seus recursos. A inteligência artificial estaria a serviço do ser humano e contribuiria para a valorização do trabalho de toda a instituição judiciária. No entanto, esse ideal de justiça que combina novas tecnologias e direitos humanos está condicionado à boa qualidade dos dados, à lealdade na utilização dessas ferramentas, à transparência no processamento de algoritmos certificados e, em qualquer caso, à preservação da liberdade de apreciação do juiz.

6. CONSIDERAÇÕES FINAIS

De fato, as novas inovações apresentam desafios legais e políticos, mas é necessário encontrar um equilíbrio entre seu uso para fins legítimos, como no caso do cumprimento de uma solicitação de assistência jurídica mútua ou de cooperação internacional formalizada entre Estados, e aqueles que podem ser considerados ilegais e uma violação da privacidade dos cidadãos. O problema crescente não o fato dessas tecnologias serem comercialmente

difundidas, mas a possibilidade de que, se forem usadas para fins de aplicação da lei, acabem sendo incorporadas em esquemas governamentais obrigatórios para a população em geral.

Existem muitas recomendações que podem ser feitas em relação ao uso de tecnologias na cooperação processual penal internacional. No entanto, primeiramente, é necessário reconhecer que existe uma via média entre proteger as expectativas razoáveis de privacidade e liberdade de expressão dos cidadãos e permitir que as autoridades estatais possam desempenhar suas funções.

Partes dessa solução pode incluir a constituição de procedimentos uniformes a serem estabelecidos e adotados para a cooperação internacional, assim como atualmente existem tratados para pedidos de assistência jurídica mútua; a autorregulação dos serviços de inteligência, tornando mais explícito o uso aceitável de tecnologias de rastreamento humano com cláusulas proibitivas embutidas; e a exigência de mandados e ordens judiciais antes da implementação e monitoramento de um indivíduo.

Um objetivo mais difícil de alcançar é o alinhamento das leis estaduais e federais dos países em relação às tecnologias e suas limitações em termos de admissibilidade de provas em um julgamento. Isso acontecerá com o tempo, à medida que mais casos internacionais forem julgados sobre a utilização de inteligência artificial e demais tecnologias em tribunais para ajudar na condenação de um indivíduo.

Tais conclusões não visam apenas resolver problemas jurisdicionais temporários, quando a polícia rastreia indivíduos através de fronteiras físicas e virtuais, mas são recomendações para um protocolo comum. Algumas das questões mais urgentes que os tribunais enfrentarão a curto prazo são em que medida usar determinados tipos de dispositivos eletrônicos para vigilância, por quanto tempo, e para monitorar que tipo de atividade. Essas questões se tornam ainda mais complexas quando inseridas em contextos internacionais.

REFERÊNCIAS

ANGE, Ange. ***Investigation numérique en informatique. Autopsie d'un ordinateur de streaming: Cas du Daily Motion***. 2016. Disponível em: https://www.researchgate.net/publication/301340151_Autopsie_d%27un_ordinateur_de_streaming_Cas_du_site_Daily_Motion . Acesso em 29 ago. 2024.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. **Promulga a Convenção sobre o Crime Cibernético**, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro

de 2001. Planalto. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm.

CALLEJÓN, Francisco Balaguer. **A Constituição do Algoritmo**. Tradução Diego Fernandes Guimarães; Rio de Janeiro - Ed. Forense, 2023. ISBN 976-65-5964-852-8.

CASTRILLÓN, Omar Danilo; CÓRDOBA, María del Pilar Rodríguez; CASTAÑO, Juan David Leyton. ***Ética e inteligencia artificial: ¿necessidad o urgencia?***. Memorias, v. 3, n. p.,2008. p. 2.Disponível em: http://www.iiis.org/CDs2008/CD2008CSC/CISCI2008/PapersPdf/C054TM.pdf. Acesso em: 20 jul. 2024

CIDRÃO, Taís Vasconcelos; MUNIZ, Antônio Walber; ALVES, Ana Abigail. A oportuna e necessária aplicação do Direito Internacional nos ciberespaços: da Convenção de Budapeste à legislação brasileira: The timely and necessary implementation of International Law in the ciberspace: from the Budapest Convention to Brazilian legislation. **Brazilian Journal of International Relations**, v. 7, n. 1, p. 66-82, 2018. Disponível em: https://revistas.marilia.unesp.br/index.php/bjir/article/view/7069. Acessado em: 29 ago. 2024.

LESSIG, Lawrence Code is Law-On liberty in cyberspace– **Harvard Magazine**, janvier 2000. Disponível em: https://law.stanford.edu/publications/code-is-law-on-liberty-in-cyberspace/. Acesso em 20 ago. 2024.

MOLEIRINHO, Pedro Manuel Sequeira Estrela. **Aplicação da inteligência artificial ao serviço da função policial**. Repositório Comum. IUM – Instituto Universitário Militar, Centro de Recursos de Conhecimento. IUM-CRC-CPOG – Trabalhos de Investigação Individual, 2021. Disponível em: http://hdl.handle.net/10400.26/38136. Acesso em 17 jul. 2024.

MONTEIRO, Cláudia Servilha; MEZZAROBA, Orides. **Manual de metodologia da pesquisa no direito**. 5. ed. São Paulo: Saraiva, 2009.

NICOLAS-GRÉCIANO, Marie. L'intelligence artificielle: nouvel outil au service de la prévention de la récidive?. **Cahiers de la sécurité et de la justice: revue de l'Institut national des hautes études de la sécurité et de la justice**, n. Hors série, p. pp. 99-107, 2021. Disponível em:www.ihemi.fr/articles/lintelligence-artificielle-nouvel-outil-au-service-de-laprevention-de-la-recidive . Acesso em: 28 ago. 2024.

OLIVEIRA JUNIOR, Ilson; SANTOS, Franck Cione Coelho dos. Inteligência Artificial e policiamento preditivo*:* possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos. **Brazilian Journal of Technology**, v. 5, n. 1, p. 030-062, 2022.

OLIVEIRA, Giovana Aleixo Gonçalves de; ÁVILA, Gustavo Noronha de. Inteligência Artificial no controle de crimes. In: XI EPCC – **Encontro Internacional de Produção Científica. Anais Eletrônico**, 22/11/2019. Disponível em: https://www.even3.com.br/anais/epcc2019/188226-inteligencia-artificial-no-controle-de-crimes/. Acesso: 19 jul. 2024.

PADILHA, Rafael et al. A Inteligência Artificial e os desafios da Ciência Forense Digital no século XXI. **Estudos Avançados**, v. 35, n. 101, p. 113-138, 2021. Disponível em: https://www.scielo.br/j/ea/a/JdKN8TBqQPCx9NhX4hL5mZR/?lang=pt . Acesso em 26 ago. 2024.

WATIN-AUGOUARD, Marc. Qui exerce l'autorité dans l'espace numérique?. **Revue Lexsociété**, 2022. Disponível em: https://hal.science/hal-03601667/document . Acesso em 20 ago. 2024.