18

Direito penal e segurança da informação: por uma teoria jurídica dos crimes informáticos à luz das ciências tecnológicas e economia política

Divo Augusto P. A. Cavadas

Docente de Ensino Superior Efetivo da Universidade Estadual de Goiás (UEG). Procurador do Município de Goiânia (GO). Advogado. Doutorando em Direito da Faculdade Autônoma de Direito de São Paulo (FADISP). Mestre em História pela Pontifícia Universidade Católica de Goiás (PUC/GO). Especialista em Filosofia e Direitos Humanos. Especialista em Direito Penal e Processo Penal. Bacharel em Ciências Jurídicas e Sociais pela Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro (FND/UFRJ). Bacharelando em Engenharia de Software pelo Centro Universitário Internacional (UNINTER).

DOI: 10.47573/aya.5379.2.83.18

RESUMO

O direito penal no século XXI é contextualizado com outras áreas do conhecimento, muitas das quais derivadas de outras ciências além da puramente jurídica. Nesse sentido, haja vista a atual quadra de desenvolvimento da revolução industrial, a segurança da informação enquanto segmento privilegiado da engenharia de software encontra azo nos crimes informáticos, cuja incidência cada vez maior no mundo fenomênico enseja a elaboração de estudos convergentes a uma teoria jurídica dos crimes informáticos. Esse é o tema do presente estudo, cujo recorte lógico envolve o estudo dos crimes informáticos à luz da interdisciplinaridade do direito penal e da segurança da informação, sob recorte geográfico dirigido à legislação brasileira sobre a matéria e recorte cronológico que envolva as primeiras duas décadas do século XXI. Logo, diante de uma metodologia exploratória e calcada em levantamento bibliográfico de obras referenciadas sobre direito penal, segurança da informação, engenharia de software e economia política, sustenta-se uma teoria jurídica dos crimes informáticos como emergência dos estudos jurídico-penais no século XXI.

Palavras-chave: direito penal. crimes informáticos. tecnologia. segurança da informação.

ABSTRACT

Criminal Law in the 21st century is contextualized with other areas of knowledge, many of which are derived from sciences other than purely legal. In this sense, given the current stage of development of the industrial revolution, Security of Information as a privileged segment of Software Engineering finds ground in computer crimes, whose increasing incidence in the phenomenal world gives rise to studies converging to a legal theory of computer crimes. This is the subject of the present study, whose logical approach involves the study of computer crimes in the light of the interdisciplinarity of Criminal Law and information security, under a geographical frame directed to the Brazilian legislation on the matter and a chronological frame that involves the first two decades of the XXI century. Therefore, in the face of an exploratory methodology and based on a bibliographic survey of referenced works on Criminal Law, Security of Information, Software Engineering and Political Economy, a legal theory of computer crimes is supported as an emergence of criminal legal studies in the 21st century.

Keywords: criminal law. computer crimes. technology. security of information.

INTRODUÇÃO

As primeiras décadas do século XXI são marcadas pelo recrudescimento dos eventos característicos da pós-modernidade não apenas como momento histórico de consequências no âmbito da sociologia, mas também como paradigma científico que influencia a elaboração de estudos no âmbito das ciências humanas e sociais aplicadas.

Nesse sentido, os fenômenos que são comuns na atual quadra do processo civilizatório e ainda permanentes na relação entre sujeitos de direito internacional público (e.g. guerras e conflitos armados) intensificam-se pelo uso da tecnologia no espectro das chamadas “guerras cibernéticas”. No âmbito interno dos Estados, entes públicos e pessoas tornam-se vítimas da

atuação de crackers que invadem dispositivos informáticos para diversas finalidades criminais especialmente ligadas à constrição patrimonial dos ofendidos.

O estudo dos crimes informáticos, portanto, não pode se limitar à interpretação da dogmática jurídica criminal de forma estanque, senão contextualizada e sob reinterpretação prospectiva com outras áreas do conhecimento diretamente ligadas ao fenômeno em testilha, o que envolve a segurança da informação como segmento privilegiado de estudo a engenharia de software, que a partir do século XXI reivindica autonomia científica doutras áreas típicas da tecnologia da informação, tais como a ciência da computação, engenharia da computação, sistemas de informação, e análise e desenvolvimento de sistemas.

Ademais, os crimes informáticos ou cibernéticos têm seu desenvolvimento alinhado à atual quadra histórica do modo de produção capitalista, na medida em que a quarta revolução industrial apresenta vicissitudes no contexto da pós-modernidade que alteram a epistemologia característica da teoria do delito, apresentando novas categorias delitivas que dialogam com uma visão crítica da dogmática jurídico-penal, da criminologia e da política criminal.

Os países de capitalismo central dedicam-se mais à pesquisa e desenvolvimento no âmbito da segurança da informação, de modo a viabilizar a proteção de dados pessoais e evitar a tutela penal repressiva. Todavia, aos países de capitalismo periférico como o Brasil a ampliação do arcabouço normativo penal torna-se política pública privilegiada, o que se crê equivocado, na medida em que a tutela preventiva administrativa incorre em maior economia de recursos do erário frente a tutela repressiva criminal.

O objeto de pesquisa do presente estudo remete-se aos crimes informáticos, previstos no Decreto-Lei Federal n. 2.848/1940 (Código Penal Brasileiro – CP/1940), e estudados pela doutrina apenas a partir dos últimos anos do século XX, nada obstante a evolução tecnológica da informática desde 1960. O recorte lógico envolve a reivindicação de uma teoria jurídica dos crimes informáticos, que se intenta comprovar; o recorte geográfico traz como foco a análise do ordenamento jurídico brasileiro; e o recorte cronológico situa-se nas primeiras duas décadas do século XXI, no espectro da pós-modernidade.

A problematização da pesquisa subjacente ao presente estudo envolve as seguintes indagações: qual o tratamento dispensado pelo ordenamento jurídico brasileiro aos crimes informáticos? É possível interpretar os crimes informáticos à luz da interdisciplinaridade com outras áreas do conhecimento, em especial a segurança da informação? É possível reivindicar uma teoria jurídica dos crimes informáticos a partir do século XXI?

O objetivo geral deste estudo é o de apresentar os crimes informáticos e a regulação de tais atos ilícitos penais no ordenamento jurídico brasileiro. Os objetivos específicos, por sua vez, são os de introduzir uma epistemologia própria da interpretação de tais delitos, bem como reivindicar uma teoria jurídica dos crimes informáticos à luz de ciências tecnológicas como a engenharia de software, em que a segurança da informação é matéria de interesse.

A hipótese sustentada neste trabalho acadêmico norteia-se pela urgência na estrutura de uma teoria jurídica dos crimes informáticos nos limites da interdisciplinaridade do direito penal, da segurança da informação e da engenharia de software, considerando a autonomia didática e científica inerente a esta última a partir do século XXI.

A metodologia aplicada à pesquisa, enfim, é de natureza exploratória e qualitativa, baseada no levantamento bibliográfico de obras referenciadas no âmbito do direito penal, segurança da informação, engenharia de software e economia política, considerando as claras repercussões que os crimes informáticos produzem na economia dos países capitalistas.

Desta forma, o presente trabalho augura iniciar o debate para maior aprofundamento posterior acerca dos crimes informáticos e de que forma podem ser interpretados à luz de uma hermenêutica multidisciplinar, interdisciplinar e com pretensão transdisciplinar, na esteira da teoria do pensamento complexo propugnada pelo filósofo francês Edgar Morin (1990).

INTERSECÇÕES ENTRE DIREITO PENAL E SEGURANÇA DA INFORMAÇÃO

O direito penal ao longo do século XX passa a receber a influência da abordagem jurídica dos interesses coletivos, difusos e individuais homogêneos, característicos da teoria geracional dos direitos humanos (cf. BOBBIO, 2004). Os interesses transindividuais passam a influenciar a teoria do delito, na medida em que o bem jurídico-penal recebe uma leitura cada vez mais contextualizada com as normas constitucionais das democracias ocidentais. Logo, sustenta-se ser o bem jurídico-penal de cariz constitucional (cf. PRADO, 2019) o referencial teórico mais seguro para a compreensão desse fenômeno, que viceja a partir do último século e promove crescente interdisciplinaridade com outras áreas do conhecimento.

Nesse ínterim, as ciências ligadas ao amplo conceito de tecnologia da informação tem amplo desenvolvimento teórico e aplicação prática ao longo do século XX, com destaque para a ciência da computação, a partir da qual originam-se gradativamente outras ciências e áreas do conhecimento tecnológico, com destaque para a engenharia da computação e engenharia de software (cf. PRESSMAN e MAXIM, 2021).

Uma das disciplinas de progressivo interesse no desenvolvimento da informática é a segurança da informação, na medida em que a proteção de dados pessoais e a privacidade dos usuários de dispositivos tecnológicos (hardware) compostos de logiciários que viabilizam a execução de programas de computador por meio de algoritmos (software).

A velocidade com que se desenvolvem as ciências tecnológicas no século XX com a consequente adaptação do direito penal a tais mudanças socioeconômicas estruturantes, e que viabilizará a teoria jurídica dos crimes informáticos, pode ser considerada um dos reflexos da quarta revolução industrial na ciência jurídica. Importante a preleção de Klaus Schwab (2016, p. 40) sobre os impactos da quarta revolução industrial aos países em desenvolvimento, em especial aqueles que não estejam próximos do desenvolvimento tecnológico (em hardware e software) esperados pelo modo de produção capitalista pós-século XXI:

> Ha um cenário desafiador para os países de baixa renda, isto e, saber se a quarta revolução industrial levara a uma grande "migração" das fabricantes mundiais para as economias avançadas, algo bastante possível caso o acesso a baixos salários deixe de ser um fator de competitividade das empresas. A capacidade de desenvolver fortes setores da indústria transformadora que sirvam a economia global com base nas vantagens dos custos e um caminho de desenvolvimento já muito utilizado para que os países acumulem capital, transfiram tecnologia e aumentem os rendimentos. Caso esse caminho se feche, muitos países terão de repensar seus modelos e estratégias de industrialização. Se e como as economias em desenvolvimento podem aproveitar as oportunidades da quarta revolução industrial será uma questão importantíssima para o mundo; e essencial que sejam feitas

> mais pesquisas e reflexões para compreendermos, desenvolvermos e adaptarmos as estratégias necessárias. O perigo e que a quarta revolução industrial poderia causar uma dinâmica de jogadas do tipo "tudo ao vencedor" entre países, bem como dentro deles. Isso causaria um maior número de conflitos e tensões sociais e criaria um mundo menos coeso e mais volátil, especialmente porque as pessoas estão hoje muito mais conscientes e sensíveis as injustiças sociais e as discrepâncias das condições de vida entre diferentes países.

Nesse sentido, a segurança da informação é disciplina própria de ciências tecnológicas como a engenharia se software, que especialmente a partir do século XXI autonomizou-se da ciência da computação e da engenharia da computação para se configurar como segmento do conhecimento e profissional próprio. É importante, nesse ponto, trazer à lume as reflexões de Carvalho e Lorena (2017, p. 168) sobre o escopo e importância da engenharia de software, o que repercutirá nas considerações a serem tecidas sobre a segurança da informação e sua relação com o direito penal e com uma teoria jurídica dos crimes informáticos:

> […] **engenharia de software** é uma disciplina de Engenharia que engloba todos os aspectos de produção de software, desde os estágios iniciais de especificação de sistemas até a manutenção do sistema depois de ele ter sido colocado em uso. Por ser uma disciplina de Engenharia, ela aplica teorias, métodos e ferramentas em que essas são apropriadas. Deve ser observado que são buscadas soluções para os problemas de produção de software, mesmo na ausência de teorias e métodos aplicáveis. As restrições existentes, financeiras e da organização são levadas em consideração no processo produtivo. A engenharia de software não se preocupa apenas com os aspectos técnicos relacionados ao desenvolvimento de software, incluindo também atividades como gerenciamento de projetos e desenvolvimento de teorias, métodos e ferramentas que auxiliem na produção de software.

Logo, para a adequada elaboração de logiciário de programa de computador baseado em algoritmos (software), há a necessidade de se cumprir um requisito de confiabilidade do sistema, o que se reputa como principal objetivo da segurança da informação. Ao se evitar a vulnerabilidade a malwares e outros softwares invasores ou nocivos, a disciplina da segurança da informação aproxima-se do direito criminal no que concerne aos delitos informáticos.

POSSIBILIDADE DE UMA TEORIA JURÍDICA DOS CRIMES INFORMÁTICOS

Os crimes informáticos são fruto da proteção de bens jurídicos transindividuais pelo direito penal, no limiar do século XX. A partir do século XXI, com o recrudescimento da pós-modernidade e suas consequências históricas, sociais, econômicas e políticas, a proteção de dados pessoais como corolário da segurança da informação torna-se uma emergência para a sociedade e o direito penal é interpretado e aplicado à luz da interdisciplinaridade de tais áreas do conhecimento.

As reflexões de Damásio de Jesus e José Antonio Milagre (2016, p. 19) sobre o predomínio de uma sociedade da informação no século XXI, nesse sentido, merecem acolhida, nos termos que seguem:

> E a sociedade da informação (ou para muitos, pós-industrial) tem, sim, seus riscos. Pode ser chamada de sociedade dos riscos. Riscos que podem ser aceitos e riscos que devem ser mitigados. E um deles está associado à criminalidade digital. Ao considerarmos que nem todo o cidadão decidiu ingressar mas lançado foi no universo digital, constitui-se presa fácil nas mãos de especialistas em crimes cibernéticos, os crackers (repise-se, e não hackers – estes, pesquisadores de segurança da informação), que exploram as intimidades dos sistemas e também dos processos desenvolvidos sobre a tecnologia da informação para a prática de delitos. Um mundo onde os crackers são os mais fortes. A tecnologia

> revela um poder imenso a programadores, profissionais de segurança e a qualquer um que conheça a fundo suas intimidades. E o grande problema é o uso deste poder para más finalidades, sobretudo em um país onde educação digital (que não se confunde com aulas de informática) passa longe das escolas. Não podemos aceitar que na sociedade da informação vigore a lei de talião, autotutela ou a lei do mais forte, mas é sabido que o Direito deve prevalecer, fazendo valer a justiça nos conflitos entre cidadãos desta sociedade digital. Faz-se preciso o mínimo de controle para fazer frente àquele que realiza uma conduta antissocial cibernética. Ser internauta não é delito, assim como ser cidadão não é infração criminal, mas ambos, internauta ou cidadão, podem praticar, sim, infrações. É cediço que, pelo princípio da legalidade, não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Ninguém pode ser responsabilizado por fato que a lei desconsidera como de relevância penal.

A compreensão de que existe uma cidadania digital ("e-cidadania") torna possível a aplicação do direito penal para proteção de bens jurídicos relevantes em tal ambiente, a que parte da doutrina considera espécie da assim intitulada quarta geração de direitos humanos (BONAVIDES, 2011), no espectro do direito à informação, resguardado pela segurança da informação.

A possibilidade de uma teoria jurídica dos crimes informáticos, nesse sentido, dialoga com a atual quadra do modo de produção capitalista, na medida em que a quarta revolução industrial traz à lume no século XXI vertiginoso desenvolvimento tecnológico, pelo que torna as pessoas cada vez mais vulneráveis a sujeitos ativos de crimes informáticos ou cibernéticos.

Acerca das nuances que caracterizam o modo de produção capitalista e o exercício do direito potestativo de punir (jus puniendi) do Estado, com reflexos no âmbito da criminologia, é importante apresentar a perspectiva da teoria da criminologia radical de Juarez Cirino dos Santos, que traz relevante aporte conceitual neste mister, em especial quanto às relações travadas entre os sistemas jurídicos e o modo de produção capitalista. Preleciona o referido jurista em obra de referência (SANTOS, 2018, p. 107):

> A Criminologia Radical trabalha com a hipótese de que a crise do Direito é determinada pela crise do capitalismo, como modo de produção de classes: as contradições internas do modo de produção rompem os limites das formas ideológicas da vida social, de modo que o Direito esgota a capacidade de "fragmentação" da solidariedade da classe trabalhadora e o Estado exaure o potencial de domínio político pelos aparelhos tradicionais de controle social. Nessa fase, a estratégia das classes trabalhadoras consiste em mobilizar lutas dentro da lei, em torno da lei e, mesmo, a despeito da lei (Picciotto, 1979, p. 172-77) e, nessas condições, a questão das formas de poder que mediatizam o domínio do capital assume a maior relevância: para as classes trabalhadoras são muito diferentes as condições da "democracia liberal" (garantia das liberdades democráticas), do "bonapartismo" (destruição da legalidade, hipertrofia do executivo, parlamento desnaturado e judiciário intimidado) e do "fascismo" (governo da força bruta e do terror policial do capital monopolista).

No contexto pós-moderno, pode-se afirmar que a profusão de agentes privados sem que haja regulamentação, ainda que branda, do ambiente virtual, poderá conduzir a um estado de arbítrio por parte das corporações que predominam em semelhante ambiente, mormente no âmbito das redes sociais, o que também viabiliza, por consequência, a ocorrência de crimes informáticos praticados de forma direta ou indireta na rede mundial de computadores.

O Brasil, nesse desiderato, adotou como política pública a regulamentação branda (sem controle estatal, de modo a se garantir os cânones do Estado democrático de direito) por meio da Lei Ordinária Federal n. 12.965/2014 (Lei do Marco Civil da Internet) e da Lei Ordinária Federal n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), além das alterações no Código Penal Brasileiro (Decreto-Lei Federal n. 2.848/1940) promovidas pela Lei Ordinária Federal n. 12.737/2012 (especialmente o crime de invasão de dispositivo informático tipificado no art. 154-A) e pela Lei Ordinária Federal n. 14.155/2021 (tipificando o delito de fraude eletrônica nos

termos do art. 171, §2º-A).

A incidência de crimes informáticos, outrossim, torna-se cada vez maior num cenário desenhado de evolução da engenharia de software baseada na inteligência artificial, em que algoritmos preditivos podem ser influenciados por softwares nocivos relacionados com a prática de tais crimes. Nesse desiderato, cabem as considerações de Guimarães (2019, p. 1.566):

> O que costuma acontecer com a máquina é que ela é "treinada" para ter uma determinada reação frente a tal signo, porém, levando em conta a possibilidade de um significado novo a partir do contexto, resta clara a enorme dificuldade de promover alguns avanços tecnológicos. A ferramenta que tem sido utilizada para a otimização dessa adaptação da máquina com as variações de significados dos signos linguísticos é a interação da inteligência artificial, com simulação de diálogos. Quanto mais os "softwares" possam ser programados para desenvolver habilidade na troca informações com o ser humano em linguagem natural, maior será sua interação.

Logo, torna-se necessária uma compreensão dos crimes informáticos mais alinhada com as diversas ciências que envolvem a atividade de tecnologia da informação, em especial a engenharia de software que tem na segurança da informação disciplina de evidente relevo. A hermenêutica, nesse sentido, como ciência da interpretação alinhada com a ciência jurídica, deve se nortear por óptica multidisciplinar, interdisciplinar e com pretensão transdisciplinar a fim de contemplar uma adequada interpretação e aplicação das normas sancionatórias por crimes informáticos.

Uma teoria jurídica dos crimes informáticos, portanto, deve passar pelo crivo das ciências tecnológicas a fim de se perfectibilizar no mundo fenomênico e teorético. As lições de Damásio de Jesus e José Antonio Milagre (2016, pp. 31-32), nesse sentido, tornam-se providenciais e alinham-se com o sustentado no presente estudo:

> Este pode ser, data venia, um dos principais erros de grande parte dos doutrinadores e legisladores sobre o tema: confundirem técnica com conduta. A falta de apoio técnico – especialistas em tecnologia e segurança da informação em setores legislativos – leva o legislador brasileiro à criação de tipos penais incoerentes. Vírus de computador não é conduta incriminável, phishing scam (dependendo da técnica empregada) pode também não ser, muito menos o sniffing. Não raro, entretanto, encontramos livros classificando tais artefatos ou técnicas como condutas incriminaveis, logo, potenciais tipos criminais! Um grande erro. […] Conhecer a técnica é fundamental para o operador do Direito. Não se pode exercer com dignidade a advocacia em direito digital sem conhecer a fundo as técnicas. Não se pode jogar todas as técnicas na mesma bacia de um suposto comportamento considerado criminoso. Muitas técnicas utilizadas por crackers descaracterizam o pretenso tipo penal. Muitas técnicas, ainda, desviam a conduta da descrita no tipo. Muitas condutas protegidas pela tutela penal não abrangem determinadas técnicas. Diga-se, muitas técnicas isoladamente praticadas não representam condutas incriminadoras. Ter tal sensibilidade é fundamental para que se evitem injustiças e para que se faça uma boa defesa em processos envolvendo crimes informáticos. Tanto para defensores como para autoridades, é mister que não se considere a máxima "o que vale é a conduta, pouco importando a técnica". Esta é a luta do advogado criminal informático: impedir as arbitrariedades do Estado, desconhecedor da informática e ansioso em penalizar cidadãos, seja como for.

A sensibilidade do jurista desconhecedor das vicissitudes características das ciências tecnológicas deve nortear sua interpretação sobre os tipos penais estatuídos pela legislação do século XXI que sanciona os crimes informáticos. Semelhantemente, a aderência da opinião de atores técnicos das ciências tecnológicas na apreciação de tais delitos em processos criminais é uma emergência a ser composta tanto no direito processual penal quanto na prática jurídica criminal.

Não basta apenas a oitiva característica do meio de prova pericial: há que se acolher a opinião de estudiosos (cientistas da computação, engenheiros da computação e engenheiros de software) desde a fase de investigação preliminar (por meio da estruturação de instituições próprias de Polícia Científica a que se reivindica autonomia frente a instituições hodiernas de Polícia Judiciária, de modo a manter-se com pretensão de imparcialidade na elaboração dos laudos periciais competentes), na medida em que os crimes informáticos apresentam nuances que os tornam diferentes da criminalidade hodierna.

CONSIDERAÇÕES FINAIS

O direito penal no século XXI encontra-se progressivamente alinhado à perspectiva da pós-modernidade, na medida em que bens e interesses transindividuais passam a ser objeto de interesse tanto em doutrina quanto em jurisprudência. A proteção de direitos humanos de terceira dimensão (na teoria de Vasak, difundida por Bobbio), e mesmo de quarta ou quinta dimensões (na teoria de Paulo Bonavides) tornam-se relevantes no âmbito teorético e da práxis jurídico-penal.

Considerando que o direito criminal deve permear uma compreensão multifacetada que envolva o que abalizada doutrina cognomina de ciência total do direito penal (cf. DIAS, 2001), sob epistemologia que contemple a dogmática jurídico-penal, a criminologia e a política criminal, os delitos informáticos ou cibernéticos despontam no século XXI como uma nova forma de criminalidade, a que pode ser categorizada como delito econômico lato sensu (cf. CAVADAS, 2018).

Os crimes informáticos, dessa forma, devem ser estudados sob hermenêutica que não se obste aos lindes da ciência jurídica, mas que dialogue com outras áreas do conhecimento, mormente aquelas ligadas às ciências tecnológicas, como a ciência da computação, a engenharia da computação e a engenharia de software, na medida em que nem todo logiciário que aplique algoritmos a programas de computador é, per se, sinal de materialidade de conduta delitiva.

Nem toda técnica empregada nos variados e dinâmicos segmentos da tecnologia da informação pode ser considerada conduta lesiva a bem jurídico penalmente tutelado, sob pena da incidência de um direito penal hipertrofiado e simbólico. O Brasil, ainda não integrado às lideranças globais na segurança da informação e desenvolvimento tecnológico, deve manter um ambiente de negócios favorável sem perda do rigor com a prática de crimes informáticos.

Logo, uma teoria jurídica dos crimes informáticos deve permear temas próprios às disciplinas típicas das ciências tecnológicas mencionadas, em especial a segurança da informação, na medida em que a proteção de dados pessoais reputa-se como manutenção da higidez da cidadania digital a todos aqueles que realizam atividades no meio virtual, o que se torna hodierno a partir das primeiras décadas do século XXI, com a expansão das atividades financeiras por bancos e outros agentes econômicos por meio do uso de aplicativos digitais.

A emergência da estruturação de uma teoria jurídica dos crimes informáticos dotada de feição própria, com princípios setoriais específicos e normas especiais, também aproximará o Brasil dos países de capitalismo central que já dispõem de parque tecnológico desenvolvido e mercado consumidor consciente de seus direitos e obrigações na cadeia de produção, bem como no mercado de consumo.

Enfim, visando a uma hermenêutica própria aplicada aos crimes informáticos que seja alinhada a ciências jurídicas e ciências tecnológicas, propôs o presente estudo a integração em maior escala do corpo técnico dessa área ao sistema jurídico, na medida em que o arcaísmo ainda predominante em setores da comunidade jurídica dificulta a compreensão de conceitos e aplicações por vezes comezinhas na área de tecnologia da informação.

Não é suficiente, pois, o mero deferimento de meio de prova pericial na instrução processual criminal, mas também é necessário o fortalecimento e estruturação das instituições de Polícia Científica de modo a viabilizar a opinião de peritos técnicos no âmbito da fase de investigação preliminar.

A autonomia de tais instituições da Polícia Judiciária, nesse sentido, garantirá a não interferência da Autoridade Policial, sujeito parcial que possui interesse na conclusão das investigações – seja pela lavratura de relatório em prol de indiciamento, seja na promoção de arquivamento ao Ministério Público.

É importante ressaltar que a Autoridade Policial no âmbito do direito processual penal é parcial no sentido apresentado, e que a pressa na conclusão da fase de investigação preliminar também revela pretensão de parcialidade, que a garantia de imparcialidade deferida ao laudo pericial da Polícia Científica afasta, o que é especialmente relevante nos crimes informáticos, realizados no ambiente virtual mas cujas repercussões também podem impactar o ambiente real.

O fortalecimento de instituições que possam reunir acervo probatório idôneo externo à pretensão punitiva dos órgãos de persecução penal é consoante a atual quadra evolutiva do modelo acusatório de processo penal, expressamente previsto no Código de Processo Penal Brasileiro (Decreto-lei Federal n. 3.689/1941) e sustentado pela doutrina (cf. TOURINHO FILHO, 2012; TÁVORA e ALENCAR, 2015). Para tanto, é necessária uma releitura das funções deferidas especialmente às instituições de Polícia Científica, de modo a autonomizá-las da Polícia Judiciária propriamente dita.

Portanto, os crimes informáticos constituem-se em categoria delitiva ancorada na pós-modernidade e com franco desenvolvimento a partir do século XXI, que exigem interpretação multidisciplinar e interdisciplinar, e que denotam as vicissitudes da atual quadra do modo de produção capitalista, sendo possível uma abordagem alinhada com a economia política para se analisar uma teoria jurídica dos crimes informáticos sob a influência das ciências tecnológicas e da economia, visto que inseridos no conceito de crimes econômicos lato sensu.

REFERÊNCIAS

BONAVIDES, Paulo. Curso de Direito Constitucional. 26. ed. São Paulo: Malheiros Editores, 2011.

CARVALHO, André C. P. L. F.; LORENA, Ana Carolina. Introdução à Computação: hardware, software e dados. Rio de Janeiro: LTC, 2017.

CAVADAS, Divo Augusto P.A.. Da distinção ontológica entre crimes econômicos em sentido amplo e estrito. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5624, 24 nov. 2018. Disponível em: https://jus.com.br/artigos/69741. Acesso em: 31 mai. 2022.

DIAS, Jorge de Figueiredo. Temas Básicos da Doutrina Penal: sobre os fundamentos da doutrina penal.

Sobre a doutrina geral do crime. Coimbra: Coimbra Editora, 2001.

GUIMARÃES, Rodrigo Régnier Chemim. A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal. Revista Brasileira de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, pp. 1555-1588, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.260. Acesso em 30 mai. 2022.

JESUS, Damásio Evangelista de; MILAGRE, José Antonio. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.

MORIN, Edgar. Introduction à la pensée complexe. Paris: ESF, 1990.

PRADO, Luiz Regis. Bem Jurídico-penal e Constituição. 8. ed. Rio de Janeiro: Forense, 2019.

PRESSMAN, Roger S.; MAXIM, Bruce R. Engenharia de Software: uma abordagem profissional. Tradução: Francisco Araújo da Costa. 9. ed. Porto Alegre: AMGH, 2021.

SANTOS, Juarez Cirino dos. A Criminologia Radical. 4. ed. Florianópolis: Tirant Lo Blanch, 2018.

SCHWAB, Klaus. A Quarta Revolução Industrial. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. 10. ed. Salvador: Juspodivm, 2015.

TOURINHO FILHO, Fernando da Costa. Manual de Processo Penal. 15 ed. São Paulo: Saraiva, 2012.